



---

# ES&S Unity 3.2.1.0 VSTL Certification Test Report for testing completed by iBeta as of November 29, 2010

Prepared for  
Election System & Software  
11208 John Galt Blvd.  
Omaha, NE 68137  
EAC Application # ESS0703

Version 1.0

Report # (V)2010-13Dec-001(A)

Trace to Standards	
NIST Handbook 150-22	
Section 5.5, 5.10.1 through 5.10.3, 5.10.5, 5.10.6	
Vol. #	Section(s) #
1	1.6.1
1	2, 3, 4, 5, & 6
1	9.6.3
2	2, 3, 4, 5, & 6
2	7.4 & 7.5.
2	Appendix B

*Test Results in this report apply to the voting system configuration tested. Testing of voting systems that have been modified may or may not produce the same test results. This report shall not be reproduced, except in full.*  
iBeta Quality Assurance was accredited for Voting System Testing. iBeta submitted intent to withdraw from the EAC program effective 12/13/10 and NVLAP program effective 12/30/10.

U.S. Election Assistance Commission

VSTL

EAC Lab Code: 0702 - Effective thru 7/16/11

NVLAP®

NVLAP LAB CODE 200749-0

3131 South Vaughn Way, Suite 650, Aurora, Colorado, 80014

Form-E: VSTL Test Report template

## Version History

Ver #	Description of Change	Author	Approved by	Date
v.1.0	Initial report	Kirby Austin Steve Brown Carolyn Coggins, Jennifer Garcia, Sridevi Jakileti Kelly Swift Kevin Wilson	Carolyn Coggins	12/13/10

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION .....</b>	<b>6</b>
1.1	UNITY 3.2.1.0 PHYSICAL & FUNCTIONAL CONFIGURATION AUDIT SCOPE .....	8
1.1.1	FAILED OR INCOMPLETE TESTING OF UNITY 3.2.1.0 AS OF NOVEMBER 29, 2010.....	9
1.2	UNITY 3.2.1.0 EXCLUSIONS .....	9
1.2.1	UNITY V.4.0.0.0 SCOPE EXCLUDED FROM UNITY 3.2.1.0.....	10
1.2.2	UNITY 3.2.1.0 OTHER EXCLUSIONS .....	10
1.3	INTERNAL DOCUMENTATION .....	10
	Table 1 Internal Documents.....	10
1.4	EXTERNAL DOCUMENTATION.....	13
	Table 2 External Documents .....	13
1.5	TECHNICAL DATA PACKAGE DOCUMENTS .....	16
1.6	TEST REPORT CONTENTS.....	16
1.6.1	VSTL PROGRAM MANUAL FORMAT TRACE.....	17
	Table 3 Trace of the Test Report to the VSTL Program Manual.....	17
<b>2</b>	<b>CERTIFICATION TEST BACKGROUND .....</b>	<b>18</b>
2.1	TERMS AND DEFINITIONS .....	19
	Table 4 Terms and Definitions.....	19
2.2	PHYSICAL CONFIGURATION AUDIT .....	21
2.2.1	PCA TDP SOURCE CODE REVIEW.....	21
2.2.2	PCA TDP DOCUMENT REVIEW AND DOCUMENT CONTENT REVIEW.....	22
2.2.3	PCA SYSTEM CONFIGURATION REVIEW .....	22
2.2.4	TRUSTED BUILD AND INSTALLATION .....	23
2.2.5	QA AND CM OBSERVATIONS AND SPOT CHECK FOR CONSISTENCY .....	23
2.3	FUNCTIONAL CONFIGURATION AUDIT.....	23
2.3.1	FCA TEST DOCUMENTATION REVIEW .....	23
2.3.2	FCA FUNCTIONAL, ACCESSIBILITY, MAINTAINABILITY, ACCURACY & RELIABILITY TESTS.....	23
2.3.3	FCA VOLUME, STRESS AND ERROR RECOVERY TESTS .....	24
2.3.4	FCA SECURITY TESTS .....	24
2.3.5	FCA HARDWARE ENVIRONMENTAL TESTS.....	24
2.3.5.1	M100 Reuse of SysTest Test Results .....	25
2.3.5.2	M650, AutoMARK VAT & DS200 Reuse of ESSUNITY3200 Test Results .....	25
2.3.5.3	Changes to the DS200-Testing In Unity 3.2.1.0 & Reuse of ESSUNITY3200 Test Results.....	25
2.3.5.4	DS200 & M100 Environmental Hardware Testing In Unity 3.2.1.0 .....	25
2.3.6	FCA TELEPHONY AND CRYPTOGRAPHIC REVIEW AND TESTS .....	25
<b>3</b>	<b>VOTING SYSTEM IDENTIFICATION .....</b>	<b>26</b>
3.1	SUBMITTED VOTING SYSTEM IDENTIFICATION .....	26
	Table 5 Voting System Name and Version .....	26
	Table 6 Voting System Polling Place and Central Count Hardware .....	26
	Table 7 Voting System EMS Software .....	26
3.2	VOTING SYSTEM TEST ENVIRONMENT .....	26
	Table 8 Voting System Hardware .....	26
	Table 9 Voting System Software .....	29
	Table 10 Voting System Technical Data Package Documents .....	31
	Table 11 Testing Software, Hardware and Materials .....	33
<b>4</b>	<b>VOTING SYSTEM OVERVIEW.....</b>	<b>35</b>
4.1	ELECTION MANAGEMENT SYSTEM- PRE VOTING CAPABILITIES .....	35
4.1.1	ELECTION DATA MANAGER (EDM) .....	35
4.1.2	ES&S BALLOT IMAGE MANAGER (ESSIM).....	36
4.1.3	HARDWARE PROGRAMMING MANAGER (HPM).....	36
4.1.4	AUTOMARK INFORMATION MANAGEMENT SYSTEM (AIMS).....	36
4.1.5	AUDIT MANAGER (AM) .....	37
4.1.6	LOGMONITOR .....	37
4.2	POLLING PLACE- VOTING CAPABILITIES .....	37
4.2.1	MODEL 100.....	37
4.2.2	INTLECT DS200 PRECINCT BALLOT SCANNER .....	38
4.2.3	AUTOMARK VOTER ASSIST TERMINAL (VAT) .....	39

4.3	CENTRAL COUNT SCANNER- Post Voting Capabilities .....	40
4.3.1	MODEL 650 CENTRAL BALLOT SCANNER (M650) .....	40
4.4	ELECTION MANAGEMENT SYSTEM- Post Voting Capabilities .....	41
4.4.1	ELECTION REPORTING MANAGER .....	41
<b>5</b>	<b>CERTIFICATION REVIEW AND TEST RESULTS.....</b>	<b>42</b>
5.1	PCA SOURCE CODE REVIEW.....	42
5.1.1	M100 C SOURCE CODE REVIEW RESULTS.....	42
5.1.2	DS200 C/C++,SCANNER-C8051 C AND MYDLL C SOURCE CODE REVIEW RESULTS.....	43
5.1.3	VAT VB. NET SOURCE CODE REVIEW RESULTS .....	43
5.1.4	HPM AND ERM COBOL SOURCE CODE REVIEW RESULTS .....	43
5.1.5	AIMS SOURCE CODE REVIEW RESULTS .....	43
5.2	PCA TDP DOCUMENT REVIEW .....	43
5.2.1	UNITY 3.2.1.0 TDP DOCUMENT REVIEW RESULTS.....	44
5.3	FCA FUNCTIONAL SYSTEM LEVEL, ACCESSIBILITY, MAINTAINABILITY, ACCURACY & RELIABILITY TESTING AND REUSE OF TESTING .....	45
5.3.1	EAC EVALUATION FOR REUSE OF THE SYSTEST LABS TESTING: M100 FUNCTIONAL, ACCESSIBILITY, MAINTAINABILITY, ACCURACY & RELIABILITY TEST RESULTS .....	45
5.3.2	REGRESSION FUNCTIONAL & SYSTEM LEVEL TEST RESULTS.....	46
5.3.3	DS200 FUNCTIONAL ENHANCEMENTS AND CHANGES TEST RESULTS .....	46
5.3.4	FCA DS200 RELIABILITY TEST RESULTS.....	48
5.4	FCA M100 VOLUME, STRESS, AND ERROR RECOVERY TESTING.....	49
5.4.1	FCA M100 VOLUME STRESS AND ERROR RECOVERY TEST RESULTS .....	49
5.5	FCA SECURITY REVIEW AND TESTING.....	50
5.5.1	FCA SECURITY REVIEW AND TESTING .....	50
5.6	FCA HARDWARE ENVIRONMENTAL TESTING.....	51
5.6.1	CHANGES TO THE DS 200 FROM THE ESSUNITY3200 CONFIGURATION .....	52
Table 12 ECOs Impacting Electrical Components or Transportation & Storage.....	52	
5.6.2	ELECTROSTATIC DISRUPTION VSS 4.8.3 TESTING ON THE M100 .....	53
5.6.3	HARDWARE ENVIRONMENTAL TESTS AND TEST RESULTS .....	53
5.7	FCA TELEPHONY AND CRYPTOGRAPHIC REVIEW AND TESTING .....	53
5.7.1	FCA TELEPHONY AND CRYPTOGRAPHIC REVIEW AND TESTS .....	53
<b>6</b>	<b>OPINIONS &amp; FINDINGS .....</b>	<b>54</b>
<b>7</b>	<b>APPENDICES: TEST OPERATION, FINDINGS &amp; DATA ANALYSIS .....</b>	<b>55</b>
7.1	APPENDIX A- VSS 2002 AND APPLICABLE VVSG 2005 CERTIFICATION TEST REQUIREMENTS.....	55
7.2	APPENDIX B: PCA SOURCE CODE REVIEW .....	122
7.2.1	REUSED SYS TEST SOURCE CODE REVIEW RESULTS .....	122
7.2.2	IBETA UNITY 3.2.1.0 SOURCE CODE REVIEW RESULTS .....	122
7.3	APPENDIX C: PCA TDP DOCUMENTATION REVIEW.....	126
7.3.1	TECHNICAL DATA PACKAGE CONFIGURATION & QUALITY ASSURANCE PRACTICES .....	126
7.3.2	PCA TDP DOCUMENT REVIEW .....	126
7.4	APPENDIX D: FCA TESTING .....	147
7.4.1	FCA FUNCTIONAL SYSTEM LEVEL, ACCESSIBILITY, MAINTAINABILITY, ACCURACY & RELIABILITY TESTING .....	147
7.4.1.1	Reuse Functional System Level, Accessibility, Maintainability, Accuracy & Reliability Test Results .....	147
7.4.1.2	Regression System Level Test Result.....	147
7.4.1.3	DS200 Functional Test Result.....	158
7.4.1.4	DS200 Reliability Testing .....	166
7.4.2	FCA VOLUME (VOLUME STRESS, PERFORMANCE AND ERROR RECOVERY) TESTING .....	169
7.4.2.1	Volume 1 Test Results .....	169
7.4.2.2	Volume 2 Test Results .....	172
7.4.2.3	Volume 4 Test Results .....	175
7.4.2.4	Volume 5 Test Results .....	177
7.4.2.5	Volume 11 Test Results .....	178
7.4.2.6	Volume 12 Test Results .....	181
7.4.2.1	Volume 13 Test Results .....	184
7.4.3	FCA SECURITY REVIEW AND TESTING .....	187
7.4.4	TELEPHONY AND CRYPTOGRAPHIC REVIEW AND TESTING .....	193
7.4.5	FCA HARDWARE ENVIRONMENTAL TESTING AND REUSE.....	194
7.5	APPENDIX E- DISCREPANCY REPORT .....	199
7.6	APPENDIX F: WARRANT OF ACCEPTING CHANGE CONTROL RESPONSIBILITY.....	309

7.7	APPENDIX G: TRUSTED BUILD & VALIDATION TOOLS UNITY 3.2.1.0 VOTING SYSTEM .....	310
7.7.1	WITNESS OF THE TRUSTED BUILD OF ERM v. 7.5.7.0, HPM v.5.7.3.0 AND MYDLL v1.1.0.2.....	310
7.7.2	WITNESS OF THE TRUSTED BUILD OF M100 v. 5.4.4.4.....	314
7.7.3	WITNESS OF THE TRUSTED BUILD OF DS200 v. 1.4.3.7 .....	315
7.7.4	WITNESS OF THE TRUSTED BUILD OF DS200 ANCILLARY v. 2.20.0.0 .....	317
7.7.5	WITNESS OF THE TRUSTED BUILD OF AutoMARK VAT v. 1.3.2097.....	319
7.7.6	WITNESS OF THE TRUSTED BUILD OF AutoMARK AIMS v. 1.3.257 .....	322
7.7.7	WITNESS OF THE TRUSTED BUILD OF DS200TOS v.1.0.2.0 .....	325
7.7.8	ES&S VALIDATION TOOLS.....	328
7.8	APPENDIX H: AMENDED TEST PLAN .....	329
7.9	APPENDIX I: STATE TEST REPORTS.....	329
7.10	APPENDIX J UNITY 3.2.1.0 IMPLEMENTATION STATEMENT .....	329
7.11	APPENDIX K UNITY 3.2.1.0 LIST OF CHANGES SUBMITTED IN UNITY 3.2.1.0.....	330

# 1 Introduction

This report is submitted to the Election Assistance Commission (EAC) by iBeta Quality Assurance (iBeta) summarizing the incomplete VSTL Certification Testing of the Election System & Software (ES&S) Unity 3.2.1.0 voting system. The results of testing completed as of November 29, 2010 to the Voting System Standards 2002 (VSS 2002) and the specific requirements of Voluntary Voting System Guidelines (VVSG 2005) are identified in [Appendix A](#). iBeta withdrew from the EAC VSTL program, effective December 13, 2010, therefore this report only identifies the status of the voting system testing as of November 29, 2010. Due to nine unresolved discrepancies, see [Section 1.1.1](#), this report does not identify that Unity 3.2.1.0 met all requirements of the VSS 2002 or the applicable VVSG 2005 requirements.

The ES&S Unity 3.2.1.0 voting system was submitted to iBeta for testing to support ES&S' application #ESS00703 (originally identified as Unity 3.0.1.0 w/ ATS 1.3) to the US Election Assistance Commission (EAC) for certification to the VSS 2002. This application incorporated the initial certification of the Model 100 Precinct Scanner. Unity 3.2.1.0 is considered an initial certification, even though it includes all the products previously certified in the EAC certification **ESSUnity3200** voting system. Any changes to the previously certified products were retested to the VVSG 2005. Previously certified products that did not change were only subjected to regression testing.

## Additions or Modifications to ESSUnity3200 Configuration in Unity 3.2.1.0

Unity 3.2.1.0 incorporates the following additions or changes to the **ESSUnity3200** certified voting system.

### Hardware and Firmware additions or enhancements to ESSUnity3200 for Unity 3.2.1.0:

- Addition of the M100 Hardware v.1.3.0 and Firmware v.5.4.4.4
- ERM v.7.5.7.0 includes a change to address Issue #104 (became #20) transferred from **ESSUnity3200** (ERM v.7.5.4.0). This change is tested to VVSG 2005 v.1:2.1.6.
- DS200 v. 1.4.3.7 includes firmware updates to address internal and field cosmetic and functional enhancements and issues identified in the **ESSUNITY3200** certified - DS200 v.1.3.10.0. Changes to the DS200 from **ESSUNITY3200** are tested to the VVSG 2005 requirements.
- Minor engineering changes on the DS200 plastic ballot bin and carry case included a new metal lock, adhesive and a washer to hold internal foam padding, rail configuration to support use with the M100.
- A hardware engineering change to a cable in the Steel Ballot Box.
- Hardware engineering changes to the DS200 to address administrative production processes, labeling, and, end of life or alternated sourcing of parts (inductors, capacitor, resistors, diodes, and LCD back light inverter),
- Include in testing the AutoMark Model A200-00 Hardware Rev. 1.1 configured with the Printer Engine Board (PEB) 1.70 Single Board Computer (SBC) 2.5, (WinCE 5.0.0.19)

### Hardware and Firmware changes to ESSUnity3200 as a result of issues found in Unity 3.2.1.0 testing:

- Hardware Programming Manager (HPM) v.5.7.3.0, changed from v.5.7.1.0 to provide a warning for an M100 system limit (#67 in [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#).)
- AutoMARK Firmware v.1.3.2907, changed from v.1.3.2906 to address a very obscure display issue in a pick-a-party primary (#138 in [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#).)

### Functional Differences in Unity 3.2.1.0:

- Updates to the work environment to permit networking of PCs running the Unity EMS applications in both a peer-to-peer and client/server configuration
- Addition of the system limits of the M100
- DS200 Cosmetic enhancements include:
  - new wording for Overvote English and Spanish warnings messages
  - number of beeps in audible alarm alerts have been customized to specific functions
  - new icons on the welcome screen and Polls Open menu
  - print the machine ID and poll number on the results and audit log reports
- DS200 Functional enhancements and issues include:
  - added a new ballot style report for Early Voting
  - expanded number of precincts on Election Day from 10 to 18

- added a override feature in the DS200 to bypass the query alerts programmed in HPM so that the query(overvoted write-in, blank ballots, etc.) is automatically set to "Accept"
- update the list of events logged to include last power on/off, check for a modem and all possible halt conditions
- disabling code for the withdrawn counterfeit sensor
- correction of scanner tolerances for a rare misread identified in the field
- new version of X-Windows to address random unexpected freezes and shut downs identified in the field (See the EAC [Voting System Technical Advisory Intermittent Freeze/Shutdowns with EAC Certified ES&S Unity 3.2.0.0 System](#))

#### Document Differences in Unity 3.2.1.0

- Unity 3.2.1.0 System Overview,
- Unity 3.2.1.0 System Limits (incorporating M100 limits)
- Unity 3.2.1.0 Windows Hardening documentation addressing networking of EMS PCs
- M100 documents
- Rebranded Unity 3.2.0.0 documents as Unity 3.2.1.0 project document
- Unity 3.2.1.0 documents to reflect cosmetic/ functional enhancement and issues encountered in testing. (Document issues are identified in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#).)

#### Unchanged configuration of ESSUnity3200 in Unity 3.2.1.0

##### Election Management System software:

- Audit Manager (AM) v.7.5.2.0
- Election Data Manager v.7.8.1.0
- AIMS (Automark information Management System) v.1.3.257 (There is no source code difference between **ESSUNITY3200** version 1.3.157 and 1.3.257, but there is a difference in Build package. "AIMS ESS Installation.ism" allows AIMS to run in a multi-user environment.)
- ES&S Ballot Image Manager (ESSIM) v.7.7.1.0
- LogMonitor v.1.0.0.0

##### Precinct Hardware and Firmware

- AutoMark Model A100-00 Hardware Rev. 1.0 Printer Engine Board (PEB) 1.65 Single Board Computer (SBC) 1.0, (WinCE 5.0.1400)
- AutoMark Model A200-00 Hardware Rev. 1.1 Printer Engine Board (PEB) 1.65 Single Board Computer (SBC) 2.0, (WinCE 5.0.1400)
- AutoMark Model A200-00 Hardware Rev. 1.3.1 Printer Engine Board (PEB) 1.65 Single Board Computer (SBC) 2.5, (WinCE 5.00.19)
- AutoMark Model A200-00 Hardware Rev. 1.3.1 Printer Engine Board (PEB) 1.70 Single Board Computer (SBC) 2.5, (WinCE 5.00.19)

##### Central Count Hardware and Firmware

- Model M650 Hardware v. 1.1, v. 1.2, Firmware v. 2.2.2.0, (QNX Kernel 4.25)

The purpose of this report is to provide an overview of the certification testing and findings completed as of November 29, 2010. The complete list of the system names, major subsystems, version numbers and any interfacing devices is detailed in [Section 3 Voting System Identification](#). Additional details of the design, structure, and processing capabilities are identified in the [Section 4 Voting System Overview](#).

#### Reuse of Unity 4.0 Testing by SysTest in Unity 3.2.1.0

Application #ESS0703 originally identified SysTest Labs (SysTest) as the VSTL. Due to the suspension of SysTest in the middle of various Unity certification efforts, ES&S was authorized by the EAC to transfer the testing supporting their application for certification of the Unity 3.2.1.0 (originally identified as Unity 3.0.1.0 w/ ATS 1.3) to iBeta. Unity 3.2.1.0 includes all the of paper ballot voting systems contained in the Unity v.4.0.0.0 voting system. At the time of the suspension the Unity v.4.0.0.0 test plan was approved by the EAC and a substantial amount of relevant testing had been successfully completed. ES&S petitioned the EAC to assess the testing performed by SysTest for consideration of reuse. The EAC issued a letter to

ES&S, 8-04-09 Ltr to ESS reuse of testing final, in which they outlined the conditions for the assessment of reuse process. This process is outlined in the as-run test plan (see [Appendix H Amended Test Plan](#)).

In the letter [03.24.10 Reuse of prior testing conducted by SysTest Laboratories](#) the EAC authorized the reuse of the functional, accessibility, maintainability, accuracy, and reliability testing conducted for the M100 based upon the EAC technical reviewer's audit of the test plans, test methods, test cases, and test results from the Unity 4.0 test campaign. This included a review of a document created by SysTest that summarized testing conducted for Unity 4.0. The EAC concluded:

- All functional, accessibility, maintainability, accuracy, and reliability testing outlined in the approved SysTest Unity 4.0 test plan is approved for reuse in the Unity 3.2.1.0 test campaign.
- As part of the remaining testing the EAC is tasking iBeta with testing and verifying that the Unity 3.2.1.0 system is in compliance with EAC RFI 2008-07 "0' count to start the election". This testing should be reflected in the test plan being developed by iBeta for the Unity 3.2.1.0 system.
- iBeta is also tasked with testing the discrepancies listed by SysTest within the application for Unity 3.2.1.0.

## 1.1 **Unity 3.2.1.0 Physical & Functional Configuration Audit Scope**

This certification test effort included a Physical Configuration Audit (PCA) and Functional Configuration Audit (FCA) of the Unity 3.2.1.0 additions to the **ESSUNITY3200** voting system. Due to the ES&S petition for reuse of the M100 testing these tasks were performed by either SysTest or iBeta. Assessment of the SysTest test results was performed by either iBeta or the EAC Technical Reviewers as instructed by the EAC in the *8-04-09 Ltr to ESS reuse of testing final*.

The Physical Configuration Audit (PCA) performed by iBeta for Unity 3.2.1.0 incorporated a:

- PCA Document Review of the additions to the **ESSUNITY3200** Technical Data Package (TDP);
- 3% PCA Source Code Review Assessment for reuse of the SysTest source code review of the Unity v.4.0.0.0 M100 source code review;
- Transfer of the unchanged **ESSUNITY3200** escrowed installations to the Unity 3.2.1.0 test platforms;
- Assessment of the engineering changes to the DS200 scanner and ballot boxes;
- Trusted Build of the M100, DS200 and VAT firmware and modified AIMS, HPM and ERM software performed by iBeta from the SysTest and iBeta reviewed source code; and
- Examination of the Unity 3.2.1.0 voting system configuration submitted to iBeta.

A Functional Configuration Audit (FCA) of Unity 3.2.1.0 included an EAC review of the Unity v.4.0.0.0 testing on the M100 performed by SysTest to:

- The requirements of VSS 2002;
- The Unity v.4.0.0.0 M100 specifications of the ES&S TDP; and
- The voting system requirements of section 301 of the Help American Vote Act (HAVA).

For the balance of the FCA iBeta identified the scope of the Unity 3.2.1.0 volume, stress, error recovery, environmental and security requirements of the VSS 2002, a sampling of VSS 2002 requirements necessary to conduct a single end-to-end system level functional regression test to incorporate the Unity 3.2.1.0 modifications to the **ESSUNITY3200** certified voting system combined with the unmodified portions of **ESSUNITY3200**, and the modifications to the **ESSUNITY3200** certified DS200. iBeta:

- Developed a Unity 3.2.1.0 test plan;
- Customized volume, stress, error recovery, security and regression test cases;
- Created DS200 Functional and Reliability test cases addressing the functional enhancements, issues identified by ES&S internal testing and issues identified by jurisdictions in the field. These were tested to the relevant requirements of the VVSG 2005;
- Managed the submitted system configurations;
- Executed these tests, and

- Analyzed the test results for the iBeta executed tests.

Certification testing performed by iBeta complied with the requirements of VSS 2002, Volume 2 Test Standards (and applicable VVSG 2005 requirements). The iBeta test record included the tests and reviews performed by iBeta. These tests and reviews included the requirements that were satisfactorily and unsatisfactorily completed, deficiencies noted, reports to ES&S, resolutions provided by ES&S, validations of resolutions and documentation of incorporation of resolutions into the voting system. Test records for work performed by SysTest were retained by them. Materials were provided to the EAC and iBeta for the assessment of reuse.

iBeta Quality Assurance, a limited liability company, is located in Aurora, Colorado. The company is a full service software testing laboratory providing Quality Assurance and Software Testing for the business and interactive entertainment communities. iBeta's accreditations for the testing of voting systems to the federal standards include

- National Voluntary Lab Accreditation Program (NVLAP) Voting System Test Lab (VSTL)
- Election Assistance Commission Voting Systems Test Lab (VSTL)

Testing performed under iBeta's purview was conducted at iBeta in Aurora, Colorado and Criterion Technology, Rollinsville, CO. Non-core hardware environmental testing is outside iBeta's accreditation scope as a VSTL. iBeta confirmed sub-contractor Criterion accreditation by the NVLAP of [the complete list of test methods for Electromagnetic Compatibility & Telecommunications valid through March 31, 2011](#).

Testing permitted for reuse from Unity 4.0.0.0 was tested at SysTest in Denver, Colorado and various SysTest subcontractor non-core hardware environmental test labs. Non-core hardware environmental testing is outside SysTest's test accreditation scope as a VSTL. SysTest's methods for validating the qualifications of the subcontractor laboratories was provided to the EAC and considered in their decision to permit reuse of the non-core environmental testing. SysTest conducted the non-core safety and hardware environmental assessments and testing with the following subcontractors:

- Compliance Integrity Services 1822 Skyway Drive Unit J, Longmont, Colorado 80504
- Criterion Technology 1350 Tolland Road, P.O. Box 489, Rollinsville, CO 80474
- Percept Technology Labs 4735 Walnut St. #E, Boulder, CO 80301
- Sun Advanced Product Testing (APT) 1601 Dry Creek Drive Suite 2000, Longmont, CO 80503

### **1.1.1 Failed or Incomplete Testing of Unity 3.2.1.0 as of November 29, 2010**

As of November 29, 2010 the Reliability test to confirm the correction of the freeze issue identified in the field was incomplete. The test was halted when discrepancy #187 was encountered. It is unclear if discrepancy #187 is a failure. The DS200 accepted a ballot that dropped into the ballot box but then reported the ballot as if it was rejected. This would not be a failure of the test if the root cause analysis of the issue confirms this was not a loss of function (see [Section 5.3.4](#)).

Four documentation discrepancies (#178, 181, 182, and 191) and five additional functional discrepancies remained unresolved (# 187, 188, 189, 190, and 192). They are all identified as "Open" with detailed descriptions in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#).

## **1.2 Unity 3.2.1.0 Exclusions**

As identified in the VSS2002 vol.1 section 4.1.2, software is excluded if it:

- Provides no support of voting system capabilities;
- Cannot function while voting system functionality is enabled; and
- Procedures are provided that confirm software has been removed, disconnected or switched.

### **1.2.1 Unity v.4.0.0.0 Scope Excluded from Unity 3.2.1.0**

The following Unity 4.0.0.0 items are excluded from the Unity 3.2.1.0 voting system submitted for Certification under EAC Application # ESS0703:

- Hardware and related software/firmware or peripherals of the: Automated Bar Code Reader (ABCR), iVotronic DRE Precinct Tabulator, the DS200 modem kit, the M100 modem functionality, and the M650 configured with a network card;
- EMS Software: Data Acquisition Manager and iVotronic Ballot Image Manager; and
- System functionality and maintenance: DRE, VVPAT
- Public network data transmission for remote transmission of votes or consolidated results
- Language accessibility other than English and Spanish.

In an email dated October 15, 2009 the EAC granted permission for ES&S to reuse the Unity v.4.0.0.0 TDP if the documents contained a disclaimer outlining the uncertified functionality that was not part of the Unity 3.2.1.0 certification. Examination of document content related to the uncertified Unity v.4.0.0.0 functionality was excluded.

In receiving the hardware, source code, documents and test artifacts from SysTest, iBeta determined if the material was in or out of the scope of Unity 3.2.1.0. Items determined to be out of scope have been returned to ES&S without further examination.

### **1.2.2 Unity 3.2.1.0 Other Exclusions**

The following functions are excluded from Unity 3.2.1.0 voting system and are not tested in this certification effort.

- Provisional ballots: The handling of provisional ballots on the M100 is procedural. There is no provisional ballot functionality.
- Transmission via Public Telecommunications: There is no transmission via public telecommunications. The M100 modem was removed from this certification.
- Use of Wireless Communications: There is no use of wireless communications.
- Enhanced AutoCast: This AutoMARK functionality requires both PEB v.1.70 and Auto MARK FW v.1.4. That version of AutoMARK firmware is not supported in Unity 3.2.1.0.
- There is no provision for the broadcasting of results.

Any activities in these areas are limited to documentation that the functions are not applicable to this voting system.

## **1.3 Internal Documentation**

The documents identified below are iBeta internal documents used in certification testing

**Table 1 Internal Documents**

Version #	Title	Abbv	Date	Author (Org.)
<b>iBeta &amp; ES&amp;S Contract Documents</b>				
v.07	Voting Certification Master Services Agreement- Election Systems & Software	MSA contract	11/15/08	iBeta Quality Assurance
Rev 01	Statement of Work No. 03 Maximum Reuse Project Estimate	SOW 3-01		iBeta Quality Assurance
Rev 01	Statement of Work No. 04 and change orders	SOW 4-01		iBeta Quality Assurance
<b>iBeta VSTL Procedures</b>				
v.3.0	Voting Deliverable Receipt Procedure		2/9/10	iBeta Quality Assurance
v.4.0	PCA Document Review Procedure		5/6/10	iBeta Quality Assurance
v.5.0	PCA Source Code Review Procedure		4/30/10	iBeta Quality Assurance
v.5.0	C and C++ Review Criteria		3/2/09	iBeta Quality Assurance
v.0.2	COBOL Review Criteria		3/3/09	iBeta Quality Assurance
v.1.0	Witness Build Procedure		4/07/08	iBeta Quality Assurance
v.3.0	Trusted Build Procedure		4/6/10	iBeta Quality Assurance
v.5.0	Test Case Preparation & Execution Procedure		2/9/10	iBeta Quality Assurance

<b>Version #</b>	<b>Title</b>	<b>Abbv</b>	<b>Date</b>	<b>Author (Org.)</b>
v.6.0	Project Management Voting Procedure		4/12/10	iBeta Quality Assurance
v.5.0	VSTL Test Planning Procedure		2/9/10	iBeta Quality Assurance
v.5.0	VSTL Certification Report Procedure		4/6/10	iBeta Quality Assurance
iBeta	Unity 3.2.1.0 Testing			
	ESS Source Code Review Assessment Letter	3% Source Code Review Assessment	8/13/09	iBeta Quality Assurance
7.5.7.0c	COBOL ERM 7.5.7.0c 06172010		7/12/2010	iBeta Quality Assurance
1.1.0.2c	C MYDLL_ 1.1.0.2c_06162010		6/16/2010	iBeta Quality Assurance
1.4.3.7a	C and C++ DS200_1.4.3.7a_11082010		11/08/2010	iBeta Quality Assurance
5.4.4.4.1	C M100 5.4.4.4.1 11012010		11/01/2010	iBeta Quality Assurance
2.20.0.0a	C Scanner_C8051 - 2.20.0.0a_12162009		12/18/2009	iBeta Quality Assurance
5.7.3.0b	Cobol HPM 5.7.3.0b 06172010		7/12/2010	iBeta Quality Assurance
1.3.2907a	VB.NET Automark 1.3.2907a VAT 04132010		4/13/2010	iBeta Quality Assurance
	Unity 3.2.1.0 PCA Document Review	PCA Document Review	8/20/10	iBeta Quality Assurance
	ESS Unity 3.2.1.0 Code & Equipment Receipt		9/17/09	iBeta Quality Assurance
	Test Methods Unity 3.2.1.0		8/10/10	iBeta Quality Assurance
	FCA Environmental Test Case Unity 3.2.1.0		7/29/10	iBeta Quality Assurance
	Regression		11/18/10	iBeta Quality Assurance
	Reliability( DS200)		11/11/10	iBeta Quality Assurance
	FCA Security Review Unity 3.2.1.0		9/4/09	iBeta Quality Assurance
	FCA Security Test - Unity 3.2.1.0 Windows Configuration Test steps		9/16/09	iBeta Quality Assurance
	FCA Telephony & Cryptographic TC Unity 3.2.1.0		9/10/2010	iBeta Quality Assurance
	FCA Test Documents Review Unity 3.2.1.0		8/4/09	iBeta Quality Assurance
	FCA Volume 1		9/4/09	iBeta Quality Assurance
	FCA Volume 2		9/4/09	iBeta Quality Assurance
	FCA Volume 4		8/27/09	iBeta Quality Assurance
	FCA Volume 5		8/26/09	iBeta Quality Assurance
	FCA Volume 11		9/16/09	iBeta Quality Assurance
	FCA Volume 12		9/17/09	iBeta Quality Assurance
	FCA Volume 13		5/04/10	iBeta Quality Assurance
	Reuse Characteristics Test Case -Unity 3.2.1.0		10/11/10	iBeta Quality Assurance
	EAC Clearing House Catalog		9/2/09	iBeta Quality Assurance
	Validated Test Tools		7/8/09	iBeta Quality Assurance
	ES&S Unity 3.2.1.0 EAC Matrix		12/13/10	iBeta Quality Assurance
iBeta	ECO Assessments DS200 Ballot Box			
	Assessment ECO000315 Add Glue to BOM		10/27/09	iBeta Quality Assurance
	Assessment ECO000332 New lock		11/19/10	iBeta Quality Assurance
	Assessment ECO000337 Status Change		9/18/09	iBeta Quality Assurance
	Assessment ECO000339 Add washer to lid		11/19/10	iBeta Quality Assurance
	Assessment ECO000342 Ballot Box Retrofit Change to Engineering Status (process)		8/11/09	iBeta Quality Assurance
	Assessment ECO000359 Ballot Box Bottom Edge		9/18/09	iBeta Quality Assurance
Rev 1	Assessment ECO 000366 Drawing Ballot Box Retrofit		8/18/09	iBeta Quality Assurance
	Assessment ECO000375 Drawing Carry Case		11/19/09	iBeta Quality Assurance
	Assessment ECO000423 Ballot Box Shipping Configuration		9/30/09	iBeta Quality Assurance
	Assessment ECO000466 Hardware used to bolt casters to ballot box		10/27/09	iBeta Quality Assurance
Rev 2	Assessment ECO000529 DS200 Carry Case- Remove Micro Switch bracket, and switch cable & Reduce glue usage during production		12/7/09	iBeta Quality Assurance

Version #	Title	Abbv	Date	Author (Org.)
	Assessment ECO000618 Part Number labels		1/19/10	iBeta Quality Assurance
	Assessment ECO 000665 Ballot Box diverter extender field retro-fit		5/11/10	iBeta Quality Assurance
	Assessment ECO 000669 Ballot tub		5/11/10	iBeta Quality Assurance
	Assessment ECO 000628 & 000674 Plastic power cord shield insert		5/11/10	iBeta Quality Assurance
iBeta	ECO Steel Ballot Box			
	Assessment ECO 836 Security pin added		10/24/09	iBeta Quality Assurance
	Assessment ECO 843 New diverter cable		11/11/09	iBeta Quality Assurance
	Assessment ECO 845 Caster inner bearing		10/24/09	iBeta Quality Assurance
iBeta	ECO Assessments DS200			
	Assessment ECO000523 Double coated tap		1/19/10	iBeta Quality Assurance
	Assessment ECO000534 Clamp to chassis		1/27/10	iBeta Quality Assurance
	Assessment ECO000535 Clamps chassis tape and holes		1/25/10	iBeta Quality Assurance
	Assessment ECO000545 Image Scanner Cable labels		1/19/10	iBeta Quality Assurance
	Assessment ECO000554 Drawings displaying Mylar tab on the image sensor		1/19/10	iBeta Quality Assurance
	Assessment ECO000562 Mount knurling motor		1/19/10	iBeta Quality Assurance
	Assessment ECO000566 Labels, screws & clamps		1/19/10	iBeta Quality Assurance
	Assessment ECO000570 isolated conductors replaced with multi-colored wires. Changed screw heads from Binding head to PHP		1/19/10	iBeta Quality Assurance
	Assessment ECO000576 EOL SMT Power Inductors		1/20/10	iBeta Quality Assurance
	Assessment ECO000582 Printer door		1/19/10	iBeta Quality Assurance
	Assessment ECO 839 (DS200 CF label)		8/20/09	iBeta Quality Assurance
	Assessment ECO 837 Changed size of thumb drive casing		10/26/09	iBeta Quality Assurance
	Assessment ECO 838 COT Change firmware in Delkin 4gb & 8gb thumb drives		10/27/09	iBeta Quality Assurance
	Assessment ECO 841 EOL Sensor, power switch & capacitor		11/20/09	iBeta Quality Assurance
	Assessment ECO 844 EOL parts changed w/Equivalent replacements/ Alternate parts		11/20/09	iBeta Quality Assurance
	Assessment ECO 846 Documented part number		10/27/09	iBeta Quality Assurance
	Assessment ECO 847 Alternate LCD backlight inverter		11/20/09	iBeta Quality Assurance
	Assessment ECO 851 USB Part Number		1/19/10	iBeta Quality Assurance
Unity	v.4.0.0.0 Reuse Correspondence			
	ESS Unity 3.2.1.0 Source Code Reuse Recommendation*		8/13/09	EAC
Reused	<b>EAC Certification # ESSUnity3200</b>			
v.4.0	Election Systems & Software Unity 3.2.0.0 Voting System VSTL Certification Test Report (V)2009-30Jun-001(D) *	ESSUNITY3200 Test Report	7/22/09	iBeta Quality Assurance
	FCA Volume 3		6/3/09	iBeta Quality Assurance
	FCA Volume 6		6/17/09	iBeta Quality Assurance
	FCA Volume 7		6/17/09	iBeta Quality Assurance
	FCA Volume 8		6/17/09	iBeta Quality Assurance
	FCA Volume 9		6/29/09	iBeta Quality Assurance
	FCA Volume 10		5/12/09	iBeta Quality Assurance
	FCA Security Review Unity 3.2		6/23/09	iBeta Quality Assurance
	FCA Security Test - Unity 3.2 Windows Configuration Test steps		6/3/09	iBeta Quality Assurance

Version #	Title	Abbv	Date	Author (Org.)
	Regression System Level TC		6/17/09	iBeta Quality Assurance

\* Public document found on the [EAC website](#)

## 1.4 External Documentation

The documents identified below include general external resources used in all certification testing. ES&S and EAC correspondence relevant to the Unity 3.2.1.0 test effort is listed. SysTest Unity 4.0.0.0 test documents are included only if they are relevant to the Unity 3.2.1.0 test effort.

**Table 2 External Documents**

Version #	Title	Abbv	Date	Author (Org.)
	Help America Vote Act*	HAVA	10/29/02	107 <sup>th</sup> Congress
NIST Handbook 150 2006 Edition	NVLAP Voting System Testing	NIST 150	Feb.2006	National Voluntary Lab Accreditation Program
NIST Handbook 150-22	NVLAP Voting System Testing	NIST 150-22	Dec. 2005	National Voluntary Lab Accreditation Program
	Federal Election Commission Voting System Standards	VSS	April 2002	Federal Election Commission
	Voluntary Voting System Guidelines	VVSG	December 2005	EAC
	Testing and Certification Program Manual*	Certification Program Manual	1/1/07	EAC
v.1.0	Voting System Test Laboratory Program Manual*	VSTL Program Manual	July 2008	EAC
v.5.2	EAC Test Matrix template*			EAC
	EAC Decision on Request for Interpretation 2007-01, Rev. 2 2005 VVSG Vol. 1 Section 3.2.2.1 (e) *	RFI 2007-01	5/23/07	EAC
	EAC Decision on Request for Interpretation 2007-02, 2002 Voting Systems Standards, Vol. 1, Section 4.2.5*	RFI 2007-02	5/14/07	EAC
	EAC Decision on Request for Interpretation 2007-04, 2005 VVSG Vol. 1 Section 3.1.3*	RFI 2007-04	10/29/07	EAC
	EAC Decision on Request for Interpretation 2007-05, 2005 VVSG Vol. 1 Section 4.2.1 (Testing Focus and Applicability) *	RFI 2007-05	11/6/07	EAC
	EAC Decision on Request for Interpretation 2007-06, 2005 VVSG Vol. 1 Section 4.1.1, 2.1.2c &f, 2.3.3.3o & 2.4.3c&d. (Recording and reporting undervotes) *	RFI 2007-06	11/7/07	EAC
	EAC Decision on Request for Interpretation 2008-01, 2002 VSS Vol. II, 2005 VVSG Vol. II, Section 4.7.1 & Appendix C*	RFI 2008-01	2/6/08	EAC
	EAC Decision on Request for Interpretation 2008-02, Battery Backup for Optical Scan Voting machines*	RFI 2008-02	2/19/08	EAC
	EAC Decision on Request for Interpretation 2008-03 (Operating System Configuration) 2002 VSS Vol. 1: 2.2.5.3, 4.1.1, 6.2.1.1, Vol. 2: 3.5; 2005 VVSG Vol. 1: 2.1.5.2, 5.1.1, 7.2.1, Vol. 2: 3.5*	RFI 2008-03	10/3/08	EAC
	EAC Decision on Request for Interpretation 2008-04, 2002 VSS Vol. I, Section 2.3.1.3.1a 2005 VVSG Vol. II, Section 2.2.1.3a Ballot	RFI 2008-04	5/19/08	EAC

<b>Version #</b>	<b>Title</b>	<b>Abbv</b>	<b>Date</b>	<b>Author (Org.)</b>
	Production*			
	EAC Decision on Request for Interpretation 2008-05 2002 VSS Vol. I, Section 3.4.2 2005 VVSG Vol. I, Section 4.3.2, Durability*	RFI 2008-05	5/19/08	EAC
	EAC Decision on Request for Interpretation 2008-06, 2002 VSS Vol. I, Sections 3.2.2.4c, 3.2.2.5 2005 VVSG Vol. I, V. 1.0, Sections 4.1.2.4c (Electrical Supply), 4.1.2.5 (Electrical Power Disturbance)*	RFI 2008-06	8/29/08	EAC
	EAC Decision on Request for Interpretation 2008-07; 2002 VSS Vol. I, Sections, 2.3.4, 2.3.5, 2.3.6, 2.4.1, 4.4.3, 9.4; 2002 VSS Vol. II, Sections, 3.3.1, 3.3.2; 2005 VVSG Vol. I, Sections, 2.2.4, 2.2.5, 2.2.6, 2.3.1, 5.4.3; 2005 VVSG Vol. II, Sections, 1.3, 3.3.1, 3.3.2*	RFI 2008-07	8/27/08	EAC
	EAC Decision on Request for Interpretation 2008-09 (Safety Testing) 2002 VSS Vol. I, Section, 3.4.8 2005 VVSG Vol. I, Section 4.3.8*	RFI 2008-09	8/25/08	EAC
	EAC Decision on Request for Interpretation 2008-10 (Electrical Fast Transient) 2005 VVSG Vol. I, Section 4.1.2.6 2005 VVSG Vol. II, Section 4.8*	RFI 2008-10	8/28/08	EAC
	EAC Decision on Request for Interpretation 2008-12(Ballot marking Device/ Scope of Testing) 2005 VVSG Vol. 1: 2.1.5. System Audit 2005 VVSG Vol. 1: 2.1.5.2 Shared Computing Platform*	RFI 2008-12	12/19/08	EAC
	EAC Decision on Request for Interpretation 2009- 001 (VVPAT Accessibility) 2005 VVSG Volume1: 7.8.2, 7.9.7*	RFI 2009-01	6/25/09	
	EAC Decision on Request for Interpretation 2009- 02 (Alternate Languages) 2002 VSS Volume I: 2.2.1.3a ballot Production 2005 VVSG Volume I: 3.1.3 Alternate Languages*	RFI 2009-02	8/45/09	EAC
	EAC Decision on Request for Interpretation 2009- 03 (Battery Back Up for Central Count) EAC Decision on Request for Interpretation 2008- 06 (Battery Back Up for Central Count) 2002 VVSS Vol I, Sections 3.2.2.4c, 3.2.2.5 2005 VVSG Vol I, Ver. 1.0, Sections 4.1.2.4c (Electrical Supply), 4.1.2.5 (Electrical Power Disturbance)*	RFI 2009-03	9/28/09	EAC
	EAC Decision on Request for Interpretation 2009- 04 (Audit Log Events) 2002 VSS Vol: 2.2.4.1, Common Standards, 2.2.5.1 System Audit 2005 VVSG Vol: 2.1.4 Integrity, 2.1.5 System Audit, 2.1.5.1 Operational Requirements, 5.4.3 In- Process Audit Records*	RFI 2009-04	9/29/09	EAC
	EAC Decision on Request for Interpretation 2009- 05 2002 VSS Vol. I, Sections, 2.2.7.2 c & d 2005 VVSG Vol. I, Sections, 3.2.2.2 c ii & iii*	RFI 2009-05	10/5/09	EAC
	EAC Decision on Request for Interpretation 2009- 06 (Temperature & Power Variation Tests) 2002 VSS Vol. I, Section 3.4.3 2002 VSS Vol. II, Section 4.7.1, 4.7.2, Appendix Sec. C.4 2005 VVSG Vol. I, Section 4.3.3	RFI-2009-06	4/6/2010	EAC

Version #	Title	Abbv	Date	Author (Org.)
	2005 VVSG Vol. II, Section 4.7.1, 4.7.3, Appendix Sec. C.4 EAC Decision on RFI 2008-1*			
	EAC Decision on Request for Interpretation 2010-01 2002 VSS Vol. I, Sections, 3.2.2.8 2005 VVSG Vol. I, Sections, 4.1.2.8*	RFI-2010-01	3/16/10	EAC
	Notice of Clarification NOC 07-001: Timely Submission of Certification Application*	NOC 07-001	7/17/07	EAC
	Notice of Clarification NOC 07-002: VSTL Work with Manufacturers Outside of Voting System Certification Engagements*	NOC 07-002	7/24/07	EAC
	Notice of Clarification: NOC 07-003: State Testing Done in Conjunction with Federal Testing within the EAC Program*	NOC 07-003	8/06/08	EAC
	Notice of Clarification: NOC 07-004: Voting System Manufacturing Facilities*	NOC 07-004	9/05/07	EAC
	Notice of Clarification 07-05: Voting System Test Laboratory (VSTL) responsibilities in the management and oversight of third party testing*	NOC 07-005	9/07/07	EAC
	Notice of Clarification NOC 08-001: Validity of Prior Non-Core Hardware Environmental and EMC Testing*	NOC 08-001	3/26/08	EAC
	Notice of Clarification: NOC 08-002: Clarification of EAC Mark of Certification Requirement*	NOC 08-002	8/30/08	EAC
	Notice of Clarification NOC 08-003: Clarification of EAC Conformance Testing Requirements for VSTLs*	NOC 08-003	7/30/08	EAC
	Notice of Clarification: NOC 09-001 Clarification of the Requirements for Voting System Test Laboratories (VSTLs) Development and Submission of Test Plans*	NOC 09-001	5/1/09	EAC
	Notice of Clarification: NOC 09-002: Clarification of EAC Laboratory Independence Requirement*	NOC 09-002	5/4/09	EAC
	Notice of Clarification NOC 09-003: Clarification of De Minimis Change Determination Requirements*	NOC 09-003	9/19/09	EAC
	Notice of Clarification NOC 09-004: Development & Submission of Test Reports*	NOC 09-004	11/9/09	EAC
	Notice of Clarification NOC 09-005: Development and Submission of Test Plans for Modifications to EAC Certified Systems*	NOC 09-005	12/2/09	EAC
Unity	3.2.1.0 EAC Correspondence			
	2002 VSS Supported Functionality Declaration		8/11/09	ES&S
	Unity 3.2.1.0 Application Letter		7/20/09	ES&S
	Unity 3.2.1.0 Application		8/11/09	ES&S
	Unity 3.2.1.0 Modules		No date	ES&S
	<a href="#">EAC Letter to ES&amp;S Granting Their Request to Change Test Labs for Unity 4.0.0.0</a>		3/9/2009	EAC
	<a href="#">03.24.10 Test Plan v.5.0. Approval.ESS Unity 3.2.1.0.FINAL</a>		3/24/10	EAC
	<a href="#">03.24.10 Reuse of prior testing conducted by SysTest Laboratories</a>		3/24/10	EAC
	<a href="#">Voting System Technical Advisory Intermittent Freeze/Shutdowns with EAC Certified ES&amp;S Unity 3.2.0.0 System</a>	Technical Advisory ES&S 2010-01	6/25/10	EAC
	<a href="#">EAC Letter of DeMinimis Changes to Unity 3.2.0.0</a>		5/25/10	EAC
	09.01.10 Approval letter of DeMinimis Changes Final		9/1/10	EAC

Version #	Title	Abbv	Date	Author (Org.)
Unity	3.2.1.0 Field Issue Freeze			
	Voting System Technical Advisory Intermittent Freeze/Shutdowns with EAC Certified ES&S Unity 3.2.0.0 System		7/1/10	EAC
	EAC expectations for freeze shut testing Letter		7/28/10	EAC
Unity	v.4.0.0.0 Reuse Correspondence			
	8 04 09 ltr to ESS reuse of testing final*		8/4/09	EAC
	9 11 09 Approval Source Code Final*		9/11/09	EAC
	03.24.10 Approval Reuse of Testing Functional FINAL		3/24/10	EAC
Unity	v.4.0.0.0 Test Documents			
Rev.10.0	ES&S Unity 4.0 Certification Test Plan Document Number 07-V-ESS-035-CTP-01		12/9/08	SysTest
Rev.0.2	Voting System Test Summary Report, Test Report for testing through 10/22/08 for ES&S Unity 4.0 Voting System, Report Number 01-V-ESS-035-CTP-01		12/19/08	SysTest
Rev.0.3	Election Assistance Commission Voting System Test Summary Report Summary of test Report for testing through 10/22/08 for Election Systems & Software (ES&S), Unity 4.0 Voting System Report Number 07-V-ESS-035-CTP-01	Summary Report of Unity 4.0	7/14/09	EAC
	Unity 4.0 Disc Rpt 10-28-08		10/28/08	SysTest
	ESS M100 Electrical Supply Rev 01 TE01		7/11/09	SysTest
	EMC Qualification Test Report Election Systems and Software Voting System, M100 Test Report Number 060530-1050		6/29/06	Criterion Technology Inc.
	Advanced Product Testing Lab Testing Services Report APT Job Number: 06-00329		7/21/06	Sun Microsystems Advance Product Testing Lab
	Certificate of Compliance Certificate Number : #SS-0806-R06-COC		7/29/08	Compliance Integrity Services
	Engineering Change Evaluation & Review ECO 682		6/28/06	SysTest
	Letter Re: Sun APT Test Report 06-00329, M100 Wireless, Testing Completed 6/6/06-6/26/06		3/3/10	SysTest

\* Public document found on the [EAC website](#).

## 1.5 Technical Data Package Documents

The Technical Data Package Documents submitted for this certification test effort are listed in [Section 3.2 Table 10](#).

## 1.6 Test Report Contents

The contents of this Test Report include:

- [Section 1](#): The Introduction- identifies the scope of certification testing.
- [Section 2](#) The Certification Test Background identifies the process for the Physical and Functional Configuration Audits.
- [Section 3](#) The Voting System Identification identifies the system configuration including hardware, software and the Technical Data Package documentation.
- [Section 4](#) The Voting System Overview identifies the overall design and functionality of voting system.
- [Section 5](#) The Certification Review and Test Results are the methods and results of the testing effort.
- [Section 6](#) The Opinions & Recommendations of the acceptability of the voting system.

Test Operations, Findings and Data Analysis are in the appendices (see [Table 3](#))

### 1.6.1 VSTL Program Manual Format Trace

[Table 3](#) traces the location of EAC required content in this report and VSS/VVSG

**Table 3 Trace of the Test Report to the VSTL Program Manual**

EAC VSTL Program Manual Appendix B		Test Report – VSS/VVSG vol. 2 Appendix B	
1.	System Identification and Overview	1. 3. 4	Introduction Voting System Identification Voting System Overview
2	Certification Test Background	2.	Certification Test Background
2.1	Revision History	2	Certification Test Background
2.2	Implementation Statement	2 Appendix J	Certification Test Background Implementation Statement
3	Test Findings and Recommendations	5	Certification Review and Test Results
3.1	Summary Finding and Recommendation	6	Opinions & Findings
3.2	Recommendation of Rejection	6	Opinions & Findings
3.3	Anomalies (may also be identified as discrepancies, issues or defects )	5  Appendices: A B D E	Provides a general description of how anomalies were encountered and reported during testing.  Appendix A traces the VVSG requirements to the specific anomalies. Addendum to Appendix B contains software related source code discrepancy detail. Appendix D Tables: "Issues Opened" traces the specific anomalies to the relevant software build. Appendix E, PCA and FCA Discrepancy Report, provides the discrepancy number, date, tester, location, description, and VSS/VVSG requirement information about anomalies encountered during document reviews and testing.
3.4	Correction of Deficiencies	5  Appendices: A B D E	Provides a general description of how deficiency corrections were confirmed.  Appendix A traces the VVSG requirements to the specific closed anomalies. Addendum to Appendix B reflects pass criteria for all reviewed source code. Appendix D Tables: "Issues Closed" traces the specific anomaly resolutions to the build Appendix E, PCA and FCA Discrepancy Report, provides the vendor responses and resolution validations for anomalies encountered during document reviews and testing.
Appendix A	Additional Findings	Appendix A	Appendix A: Certification Test Requirements contains "should" and "not applicable" requirements. Comments provide rationale and references to relevant EAC Interpretations or Notices of Clarification.
Appendix B	Warrant of Accepting Change Control Responsibility	Appendix F	Warrant of Accepting Change Control Responsibility
Appendix C	Witness Build	Appendix G	Trusted Build and Validation Tools documents the Witness of the Trusted Build
Appendix D	Test Plan	Appendix H	Test Plan
Appendix C	State Test Reports	Appendix I	State Test Reports

## 2 Certification Test Background

The ES&S Unity 3.2.1.0 incorporates the initial certification of the Model 100 precinct based paper ballot scanner added to the previously EAC certified products of the **ESSUnity3200** voting system. The changes to the system are listed in [section 1 Introduction](#) under "Additions to **ESSUnity3200** Configuration in Unity 3.2.1.0"

- Following the circumstances outlined in section 1, the scope of the ES&S Unity 3.2.1.0 certification test effort resulted in a unique set of pre-certification test activities. The purpose of these activities was to assist the EAC in determining what certification testing and reviews performed by SysTest could be reused. Responsibility for these activities was designated to either iBeta or the EAC. These activities are identified in the [section 1 Introduction](#).
  - Assessment and determination of the reuse of the Functional, Usability, Accessibility, Maintainability, Accuracy and Reliability testing of the M100 was provided by the EAC. (see [section 2.3.2](#) and [section 5.3.1](#))
  - Details and the results of the Physical Configuration Audit (PCA) and Functional Configuration Audit (FCA) pre-certification test activities performed by iBeta are provided below in sections [2.2](#) and [2.3](#).
- After the determination of reuse, the EAC issued instructions. This identified that iBeta was to only test the M100 for conformance to the 2002 VSS for the Volume, Stress, Error Recovery, Telecommunication and Security requirements. iBeta reviewed the test documentation provided by ES&S and SysTest to assess the scope of this testing.
- During the testing ES&S and the EAC expanded the scope of the Unity 3.2.1.0 certification test effort. (See [Section 2.3.2](#) ).
  - In January of 2010 ES&S submitted functional changes and enhancements for the DS200. As the DS200 was previously certified in Unity 3.2.1.0 these changes required testing to the VVSG. The EAC accepted the updated application and additional DS200 Functional test scope.
  - In April of 2010 the issue involving the DS200 Intermittent Freeze/ Shut Down (see [Technical Advisory ES&S 2010-01](#)) was identified. The EAC directed ES&S to address this issue in Unity 3.2.1.0. Changes submitted by ES&S resulted in additional DS200 Functional and Reliability testing. (A full description is in [Appendix H - Amended Test Plan](#)).
  - In September of 2010 the EAC issued an instruction to iBeta "*The Unity 3.2.1.0 test campaign is a test campaign that is testing the Unity 3.2.1.0 suite end-to-end. It is not a modification of an already certified system. There are no items within the Unity 3.2.1.0 system that are "out of scope" for testing as the entire system is being tested end-to-end. However, the EAC also recognizes that a large portion of the Unity 3.2.1.0 system has been tested and certified by the EAC as part of the 3.2.0.0 certification. Because of this the EAC has already recognized a large portion of the Unity 3.2.0.0 campaign as being applicable to Unity 3.2.1.0. Despite this allowance it is still incumbent on the EAC to fully evaluate the Unity 3.2.1.0 system especially given the already known field issues experienced by the Unity 3.2.0.0 system. Therefore, EAC instructs iBeta to examine the 27 error conditions that cause system halts per ES&S's system documentation and test to make sure each of these halts is properly handled per the standard. If iBeta feels this has been tested already iBeta may provide evidence of this for the EAC to review and accept or reject.*" This resulted in additional DS200 documentation and a review of system halt source code.

As part of the EAC Certification application ES&S provided an implementation statement for Unity 3.2.1.0 to the EAC.

Certification testing of the ES&S Unity 3.2.1.0 included PCA Reviews and FCA Testing. The evolution of testing is described in Sections 2.1.1.3 and 4.5 of [the ESS Unity 3.2.1.0 approved test plan \(v.5.0\)](#)

Daily status reports were sent to ES&S Unity 3.2.1.0 certification management staff and iBeta project test staff until iBeta's withdrawal as a VSTL. These reports included project activity status, issues, and other relevant information. Periodic status calls were held with the EAC, EAC Reviewers and ES&S. Upon request, iBeta provided the EAC with information to clarify the testing, the test process, schedule and status reports.

## 2.1 Terms and Definitions

The Terms and Definitions identified below are used in this certification test effort.

**Table 4 Terms and Definitions**

Term	Abbreviation	Definition
Absentee Ballot		A paper ballot cast outside of an early voting center or election day polling place
Adobe Acrobat Standard v.8 & v.9		COTS software used in ESSIM for creation of Portable Document Format (PDF) ballot files.
Audit Manager	AM	A Unity election management system audit logging software application for the Election Data Manager and Ballot Image Manager
Ballot Control - Accepts		HPM option that instructs the DS200 to accept and tabulate overvoted, blank, primary crossovers or ballots with unreadable marks without alerting the voter.
Ballot Control- Query		HPM option that instructs the DS200 to return and query the voter when encountering an overvoted, blank, primary crossovers or ballots with unreadable marks. Voter has the option to request a new ballot or instruct the system to accept the ballot as is.
Ballot Control - Reject		HPM option that instructs the DS200 to automatically reject crossover, overvoted or blank ballots. Ballots will not be accepted.
Ballot Marking Device	BMD	A device that marks a paper ballot for a voter
Ballot On Demand	BOD	An optional operating mode in ESSIM that is used to print a small quantity of election quality ES&S paper ballots on a COTS OKI 9600 HDN color laser printer.
Certified Information System Security Profession	CISSP	A certification for information system security practitioners, indicating successful completion of the CISSP examination administered by the International Information Systems Security Certification Consortium
Central counter		A type of voting system that records and reports paper ballots at the central count
Double Spit and Wipe		Functionality on the VAT to support older ES&S optical and digital scanners outside the scope of <b>ESSUNITY3200</b>
Early voting mode -		A mode on the DS200 that permits ballots to be cast prior to election day. A flag is set in HPM to include all precincts for the election. The poll-worker can select a voter's precinct and ballot style when used in Early Voting or an Absentee configuration.
Election Data Manager	EDM	A Unity election management system software application to define and store jurisdiction election data
Election Systems and Software	ES&S	Manufacturer of the Unity Voting System
Election management system	EMS	The ballot preparation and central count portions of a voting system.
Election Reporting Manager	ERM	A Unity central count software application to compile and report election results from Unity voting devices
Enhanced AutoCast		Functionality for automatically dropping AutoMARK ballots into a ballot box. This functionality requires PEB FW v.1.70 and Auto MARK FW v.1.4. That version of AutoMARK firmware is not supported in Unity 3.2.1.0
Escrow Agency		EAC identified repository that retains the file signature of the trusted build
ESSUnity3200		The EAC certification number of the Unity 3.2.0.0 voting system
ES&S AutoMARK Information Management System	AIMS	A windows-based election management system software application to define election parameters for the VAT, including functionality to import election

<b>Term</b>	<b>Abbreviation</b>	<b>Definition</b>
		definition files produced by the Unity EMS and create VAT flash memory cards
ES&S Ballot Image Manager	ESSIM	A Unity election management system desktop publishing tool to layout and format paper ballots
Executable Lines of Code	eLOC	Lines of code that execute functionality. Comments and blank lines are excluded from counts of executable lines of code.
Flash Memory Card	FMC	Portable memory that contains the election definition to display the ballot content on a VAT.
Full or New Code Review		First time submission submitted for certification review or previously certified code with changes to the code so significant that a full review is warranted.
Graphical User Interface	GUI	A method of interaction with a computer which uses pictorial buttons (icons) and command lists controlled by a mouse
Hardware Programming Manager	HPM	A Unity election management system software application to import, format, and convert an election file and create election definitions for ballot scanning equipment
Help America Vote Act	HAVA	Legislation enacted in 2002 which includes creation of the EAC, federal voting standards and accreditation of test labs
intElect DS200	DS200	A Unity Voting System precinct count digital scanner paper ballot tabulator including a 12-inch touch screen display providing clear voter feedback and poll worker messaging.
Model 100	M100	A Unity Voting System precinct-based, voter-activated paper ballot tabulator.
Model 650	M650	A Unity Voting System central count high-speed optical scanner paper ballot tabulator The M650 prints results reports to an external printer and saves results to a zip disk.
National Standard Reference Library	NSRL	Part of NIST that provides software escrow.
National Voluntary Laboratory Accreditation Program	NVLAP	Part of NIST that provides third-party accreditation to testing and calibration laboratories.
Open Primary Pick a Party (Party Preference)		Ballot contains all contests that the voter is eligible to vote for in addition to any nonpartisan contests. Voter only votes the partisan contests for one party but chooses which party in the privacy of the voting booth by only voting for candidates from the desired party. Pick a Party is where a party selection contest appears before the partisan section of the ballot. If the voter chooses a party from the party selection contest, votes for candidates that represent any other party are ignored so that the voter cannot spoil the ballot.
Peer-to-peer configuration	P2P configuration	The Unity configuration where the election management applications are loaded on two or more networked PCs; one of the PCs acts as the server.
Precinct counter		A type of voting system that records paper or electronic ballots at the polling place
Printer Engine Board version	PEB v.	The version of the firmware on the Printer Engine Board identifies support or non-support of Enhanced AutoCast and Double Spit & Wipe (v.1.70 supports)
Single Board Computer version	SBC v.	Version of the Single Board Computer identifying board connections and chips
Stand-alone configuration		The Unity configuration where all election management applications are loaded on a single PC
Trusted Build		A compile and build of the source code reviewed by iBeta into executable code. Construction of the build platform and compile is performed by iBeta following

Term	Abbreviation	Definition
		the documented instructions of the manufacturer. A manufacturer's representative is present to witness the build.
Technical Data Package	TDP	The documentation and code relating to the voting system, submitted by the manufacturer for review.
Universal Power Supply	UPS	Uninterrupted power supply
U.S. Election Assistance Commission	EAC	U.S. agency established by the Help America Vote Act of 2002 to administer Federal elections.
Voluntary Voting System Guidelines	VVSG	Federal voting system test standards created by the EAC. Eventually these will replace the VSS.
Voting System Standards	VSS	Federal voting system test standards, predecessor of the VVSG.
Voting System Test Lab	VSTL	Lab accredited by the EAC to perform certification testing of voting systems.
Voting Variations		Significant variations among state election laws incorporating permissible ballot content, voting options and associated ballot counting logic
Voter Assist Terminal	VAT	A ballot marking device to assist multilingual voters and voters with visual, aural or dexterity disabilities to vote a paper ballots in a private manner
Unity x.x.x.x		A voting system produced by ES&S configured with various election software applications, DREs, optical and digital scanners and ballot marking devices. The configuration varies for each version of Unity.
Unity 3.2.0.0 voting system		The ES&S EAC certified voting system including ERM, ESSIM, HPM, ERM, LogMonitor, Audit Manage, the DS200 Precinct Scanner, AutoMARK VAT Ballot Marker and M650 Central Scanner
Unity 3.2.1.0 voting system		The ES&S EAC voting system including all products of <b>ESSUNITY3200</b> , the M100 precinct scanner and EMS networking in a peer-to-peer or Windows 2003 Server configuration.
Unity 4.0.0.0 voting system		The ES&S certification testing effort submitted to SysTest which was not completed. It incorporated the products of Unity 3.2.1.0 and the iVotronic DRE. Some of the test results are authorized by the EAC for reuse in iBeta testing of <b>ESSUNITY3200</b> and 3.2.1.0.
Windows 2003 Server configuration	Server configuration	The Unity configuration where the election management applications are loaded on a server networked to one or more client PCs.
Witness Build for Unity 3.2.0.0		The Unity 4.0.0.0 Trusted Build performed by SysTest. iBeta shall initiate testing with this build. Following iBeta's performance of the Trusted Build a regression test will be run.

## 2.2 Physical Configuration Audit

The Physical Configuration Audit (PCA) deals with the physical elements of the voting system, including the source code, documentation and system configuration reviews. Additionally the Trusted Build with the reviewed source code and installation of the executable are part of the PCA.

### 2.2.1 PCA TDP Source Code Review

There were three categories of source code in Unity 3.2.1.0. Each was handled in a different manner.

- The first is code that is unchanged from the EAC certified **ESSUNITY3200** voting system. No code review was required. The **ESSUNITY3200** escrowed executables were transferred for use in testing.

- The second are source code changes submitted for certification in Unity 3.2.1.0 or changes submitted to address issues encountered during testing. All changes to code were 100% reviewed by iBeta to verify conformance to the coding requirements of VSS Vol. 1 Sect. 4.2 and Vol. 2 Sect. 5.4. The results of the review to these standards were recorded on Source Code Review sheets (Excel spreadsheets). Any issues identified in the review were logged on the *Unity 3.2.1.0 Source Code Discrepancy Report*. The report was forwarded to ES&S for correction of the code. ES&S responses and any changes were validated in a second review.
- The third is the M100 source code that had been previously reviewed by SysTest for which ES&S petitioned for reuse of this review. In order to assist in making a determination of reuse the EAC instructed iBeta to audit 3% of the source code for assessment and recommendation of reuse of the applicable M100- PCA Source Code Review conducted by SysTest in the Unity 4.0 test effort (*04 09 Itr to ESS reuse of testing Final*). iBeta focused the review on source code files and functions that process vote data, audit logs, and reporting. In assessing code iBeta reviewed the sampling using the same method used in a 100% review. Following a peer review issues were identified as:
  - Green: Non-logic issues - recommend for reuse per EAC instruction letter;
  - Yellow: Potential logic issues- attach issues to the recommendation letter to the EAC for their consideration in determination of reuse; and
  - Red: Confirmed logic issues - recommend 100% review to the EAC.

Additional information and results of the source code review are provided in [Section 5.1](#).

(**Note:** Special reviews of source code for security or other functional reasons are FCA tasks that are incorporated into an applicable test case. These reviews and results are not documented in the PCA Source Code Review but rather in the relevant FCA test case and results.)

### **2.2.2 PCA TDP Document Review and Document Content Review**

There are two types of document reviews in the certification test process.

- The first is performed to verify the presence of the document content identified in the Vol. 2 Sect. 2 requirements of the VSS. This review was conducted on the M100 TDP and Document Differences in Unity 3.2.1.0 (see [Section 1 Introduction](#) for the list of document differences). Review results were recorded on PCA TDP Document Review sheets (Excel spreadsheets). Issues were identified in the review and logged on the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#). This report was forwarded to ES&S for correction. ES&S' responses and any changes were validated in a second review. ES&S submitted a complete set of TDP documents that were substantially unchanged from the EAC certified **ESSUNITY3200** voting system. The only change was to the Unity version reference. It was changed from Unity 3.2.0.0 to Unity 3.2.1.0. iBeta performed a document comparison to confirm that there were no other significant changes to the documents. Unchanged documents required no additional review.
- The second review type is a more in depth review of the accuracy of the document content. This document review was conducted on the Unity 3.2.1.0 documents needed to complete the trusted builds, the source code review; security review, test planning, and test execution. These document reviews occurred as part of these specific tasks. They were recorded in the daily status and the applicable task documentation.

Missing content or discrepancies from either type of review were reported in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#). This report was forwarded to ES&S for correction. ES&S responses and any changes were validated in a subsequent document review. Four document discrepancies remain open on the report. Additional information and results of the document reviews are provided in [Section 5.2](#).

### **2.2.3 PCA System Configuration Review**

The PCA System Configuration Review of Unity 3.2.1.0 was performed to verify the voting system documentation and components comply with the identification requirements of the VSS Vol. 1 Sect. 8.7.1. Reviewed results are recorded on PCA System Configuration Review sheets (Excel spreadsheets). If an issue was identified in the configuration review it was logged on the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#). After completion of a peer review, the report was forwarded to ES&S for correction. ES&S responses and any changes were validated in a second review and reflected in the report.

#### **2.2.4 Trusted Build and Installation**

The Trusted Build and Installation of the executable code for the Unity 3.2.1.0 voting system was performed using the reviewed source code per the VSS Vol. 1 Sect. 9.6.2.4 (and VVSG Vol. 2 Sect 1.8.2.4 as applicable to changes). Observation of the Trusted Build by ES&S was documented in the Witness of the Final Build and Code Comparison (Word Document). The record of the final builds used in testing is found in [Appendix G](#).

#### **2.2.5 QA and CM Observations and Spot Check for Consistency**

The PCA Document Review includes a review of the ES&S Quality Assurance and Configuration Management policy and process documentation for compliance to Vol.2 Sect.2 of the VSS. iBeta checked for consistency with the policy and process in two ways.

- When receiving materials from ES&S iBeta confirmed that delivered materials were consistent with ES&S version control policies. I
- iBeta conducted a random “spot check” of this process by requesting work products for a specific engineering change from ES&S. The iBeta reviewer selected an engineering change and requested 10 work product documents or artifacts to be delivered within 24 hours. These requested materials traced this change through the ES&S system. The reviewer assessed if the materials were consistent with the policy.

Any inconsistencies were logged in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#) as “Informational”. Additional information and results of iBeta’s QA and CM assessments are provided in [Section 5.2](#).

### **2.3 Functional Configuration Audit**

The Functional Configuration Audit was an examination of the functional aspects of the voting system. This included review of the Unity 3.2.1.0 submitted test documentation and execution of the VSS 2002 required tests.

#### **2.3.1 FCA Test Documentation Review**

The FCA Test Documentation Review assessed the level of prior ES&S testing of the voting system to the VSS Vol. 1 Sect. 2, 3, 4, 5, 6, 7 and 9 requirements. This assessment was used to define the extent of functional testing required in Unity 3.2.1.0. iBeta identified and separated the scope of the required Unity 3.2.1.0 testing into two groups.

- The first group included the prior SysTest M100 test results. ES&S petitioned for reuse of SysTest’s Unity v.4.0.0.0 testing for the M100 in the Unity 3.2.1.0 test campaign. Pending a determination of reuse by the EAC, iBeta identified any open M100 discrepancies from the SysTest testing and imported them into the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#) for inclusion in the Unity v.3.2.1.0 testing.
- The second group included the testing M100 security, M100 system limits, the addition of a networked EMS, changes to ERM, and changes to the DS200 from **ESSUNITY3200**. These were identified as the scope of testing for Unity 3.2.1.0 to be performed by iBeta.

#### **2.3.2 FCA Functional, Accessibility, Maintainability, Accuracy & Reliability Tests**

Functional, Accessibility, Maintainability, Accuracy and Reliability testing on the M100 was performed by SysTest Labs. ES&S petitioned the EAC for reuse. The EAC Technical Reviewers reviewed the Functional, Accessibility, Maintainability, Accuracy, and Reliability test summary reports provided by SysTest on M100. The EAC approved the reuse of this testing to the requirements in Vol.1 Sect. 2, 3 and 4.4 (excluding the out of scope DRE specific requirements), in accordance with Vol. 2 Sect. 6. A statement regarding testing is provided by the EAC in [Section 5.3.1](#).

iBeta conducted a single regression end-to-end mock election to demonstrate the integrated functionality and processes of the ES&S Unity 3.2.1.0 for a sampling of Vol. 1 Sect. 2, 3 and 4.4, in accordance with Vol. 2 Sect. 6. Additionally the M100 Volume suite of tests generally incorporated end-to-end mock elections.

Issues that remained open from the SysTest testing were incorporated into the Regression, Volume or Security tests.

DS200 firmware updates to address internal and field cosmetic and functional enhancements and issues were tested in the DS200 Functional Test Case, with multiple test scenarios, and the DS200 Reliability Test Case. DS200 and ballot box hardware engineering change orders were incorporated into the Regression or Functional test configuration.

Issues encountered during the regression, functional or reliability testing were identified in the test record and logged on the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#). ES&S resolved all but three discrepancies. The submitted fixes were validated and recorded in the report. The three unresolved functional discrepancies (187, 188 & 192) remain “Open” on the discrepancy report.

Additional information and results of testing are provided in [Section 5.3](#).

### **2.3.3 FCA Volume, Stress and Error Recovery Tests**

iBeta reviewed the ES&S System Limitations Unity 3.2.1.0 document to identify relevant M100 limits. (As the system limits previously tested in **ESSUNITY3200** were not impacted by any of the changes submitted in Unity 3.2.1.0, no additional testing was required.) Based upon the system and application limits identified in this document iBeta defined and conducted a set of seven test cases with single or multiple scenarios. These test cases incorporated end-to-end mock elections to demonstrate the ability of the M100 to operate at the declared limits. Additional scenarios were incorporated into the test cases to demonstrate the M100’s ability to provide an appropriate response to an overloading condition exceeding the limits and recover without losing vote data. Issues encountered during testing were identified in the test record and logged on the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#). ES&S resolved discrepancies of the VSS2002. All submitted fixes were validated and recorded in the report.

### **2.3.4 FCA Security Tests**

iBeta performed a security review of the ES&S security documentation addressing Vol. 1 Sect. 2.2.1, 2.2.3, 2.2.5 and 6 and Vol. 2 Sect. 6.4. Based upon this review security specific tests were identified. These tests incorporated source code and document reviews. Functionality to meet the requirements incorporated secrecy, integrity, system audit, error recovery or access to the voting system. The review was either conducted or peer reviewed by an iBeta CISSP staff member. The tests or reviews to validate the security of Unity 3.2.1.0 were recorded in the FCA Security Review and Test Method and FCA Security Test Case Unity 3.2.1.0. Issues encountered during testing were identified in the test record and logged on the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#). ES&S resolved all but two functional discrepancies. The two unresolved security discrepancies (189 & 190) remain “Open” on the discrepancy report. All submitted fixes were validated and recorded in the Discrepancy Report.

### **2.3.5 FCA Hardware Environmental Tests**

ES&S Unity 3.2.1.0 consists of the M100 precinct count scanner, DS200 precinct count scanner, M650 central scanner and the AutoMARK VAT ballot marking device. Unity 3.2.1.0 certification test effort is the initial submission of the M100. All other hardware was previously certified in **ESSUNITY3200**.

- The M100 was part of the Unity 4.0.0.0 project, which was originally submitted for EAC certification to SysTest. SysTest’s certification was suspended by the EAC on October 29, 2008 with projects transferring to iBeta. The M100 hardware environmental testing had been completed by SysTest.
- The M650 and AutoMARK VAT hardware was unchanged from the **ESSUNITY3200** certified voting system
- ES&S submitted engineering changes for the DS200 from the **ESSUNITY3200** certified voting system. As the DS200 was previously certified in **ESSUNITY3200**, any submitted modifications that required testing were tested to the VVSG 2005.

FCA Hardware Environmental Tests are non-core tests that must be performed by a laboratory accredited in the hardware environmental test methods identified in the VSS 2002 Vol.1, Sect. 3.2.2 Environmental Requirements and VVSG 2005 Vol. 1, Sect. 4.8. Non-core tests may be performed by subcontractor laboratories, under the supervision of the VSTL, if the VSTL does not hold these accreditations. The SysTest’s subcontractors listed in the [section 1 Introduction](#) performed the hardware testing of the Unity v.4.0.0.0 voting system to the requirements of Vol.1 Sect. 3 in accordance with Vol.2 Sect. 4. Additional

hardware environmental testing was performed under iBeta's direction by Criterion Technology of Rollinsville, Colorado. Criterion's accreditation to perform all required hardware environmental tests was verified by iBeta prior to contracting.

#### **2.3.5.1 M100 Reuse of SysTest Test Results**

As the M100 was unchanged from the hardware tested by SysTest, ES&S petitioned the EAC for reuse of the M100 test results. The EAC issued their approval for reuse of the results of the SysTest Environmental Hardware testing for the M100 precinct count scanner in the *8-4-2009 Letter to ESS*. In accordance with the EAC's instructions, iBeta reviewed the SysTest reports to confirm that any failures resulting in engineering changes had been documented and the reports identified that all hardware ultimately passed. The review conducted by iBeta found four errors or omissions in the SysTest provided reports. These were documented in the [\*Unity 3.2.1.0 PCA and FCA Discrepancy Report\*](#) issues 1, 2, 27, and 28. Discrepancies 1 and 2 concerned detail missing from the v.1:4.1.2.8 Electrostatic Disruption test that was required to be run per EAC NOC 08-001 *Validity of Prior Non-Core Hardware Environmental and EMC Testing*. ES&S withdrew their request to reuse the SysTest ESD report identified in discrepancies 1 and 2. iBeta initiate an ESD test on the M100 in order to reuse the SysTest reports.

#### **2.3.5.2 M650, AutoMARK VAT & DS200 Reuse of ESSUNITY3200 Test Results**

The M650 and AutoMARK VAT were part of the **ESSUNITY3200** certified voting system. iBeta confirmed that as no change had been made to this hardware since certification, no new hardware environmental testing was required. The reused test results can be found in the **ESSUNITY3200** Test Report.

#### **2.3.5.3 Changes to the DS200-Testing In Unity 3.2.1.0 & Reuse of ESSUNITY3200 Test Results**

The DS200 was part of the **ESSUNITY3200** certified voting system. A total of 38 engineering change orders to the DS200 and ballot boxes were submitted during the Unity 3.2.1.0 certification test effort. A preliminary review of the submitted ECO's found 11 ECOs impacted the electrical tests. None of the changes impacted the transportation and storage tests. The 11 ECOs were sent to Criterion, an electrical test lab, for expert assessment. [\*Section 5.6.1 Changes to the DS200 from the ESSUNITY3200 Configuration\*](#) contains the individual results of each ECO assessed by Criterion. Six ECOs required retesting. This resulted in all EMC Operating Tests being rerun. As these were modifications to the previously certified **ESSUNITY3200** system, the testing was to the VVSG 2005. As the submitted changes did not impact the test results of the **ESSUNITY3200** certification Non-Operating Transportation and Storage Tests, those results were reused and are found in the **ESSUNITY3200** Test Report.

#### **2.3.5.4 DS200 & M100 Environmental Hardware Testing In Unity 3.2.1.0**

Environmental hardware testing was required for the DS200 and M100 as identified above. A detailed test case with test instructions was prepared by iBeta to document the assessment and testing of the DS200 and M100. A copy of the test case was provided to Criterion. iBeta created test election databases for all operating tests and to validate the operational status of the equipment before and after each environmental test. The system configuration, test objective, test steps, and expected results were identified. iBeta observed testing by Criterion and recorded the acceptance and rejection results for each test step. Criterion recorded individual test results in their internal test plan/test case. No issues were encountered during testing. In addition to the iBeta test record, Criterion provided iBeta with test reports for the DS200 and M100 following their internal processes.

### **2.3.6 FCA Telephony and Cryptographic Review and Tests**

An examination of the M100 scanner was conducted to confirm that it did not contain wireless technology or use of the public networks. The results of this review were recorded in the FCA Telephony and Cryptographic Test Case. As a result of this review it was determined that the voting system is exempted from the wireless and public network Telephony and Cryptographic requirements of VSS Vol.1 Sect. 5 & 6. Jurisdiction connection of the any Unity 3.2.1.0 voting equipment or election management system PCs or laptops to a public network or a private network (other than the Peer-to-Peer and Windows 2003 Server configurations) would not be covered by the Unity 3.2.1.0 certification.

### 3 Voting System Identification

The identification of the ES&S Unity 3.2.1.0 submitted for certification is ultimately documented by the EAC. Per their instructions the system identification is found in the *EAC Scope of Certification*. The hardware, software and the Technical Data Package documentation used in the certification test environment is identified in section 3.2.

#### 3.1 Submitted Voting System Identification

**Table 5 Voting System Name and Version**

Voting System Name	Version
Identified in the EAC Scope of Certification	

**Table 6 Voting System Polling Place and Central Count Hardware**

Hardware	OS or Firmware & Version	Description
Identified in the EAC Scope of Certification		

**Table 7 Voting System EMS Software**

Software Applications	Version	EMS Function Description
Identified in the EAC Scope of Certification		

#### 3.2 Voting System Test Environment

The Voting System Test Environment identifies the specific hardware and software that was used in the test environment. The Test Methods in Appendix D identify the specific ES&S Unity 3.2.1.0 voting system software and firmware used in each test.

**Table 8 Voting System Hardware**

Hardware or Equipment	Manufacturer	Version	Description (identify COTS)
EMS - Client/Server Configuration Optiplex 760 SN: 3x6fk1 Monitor: SN: MX-04D025-47605-1B8-DGQA Keyboard: SN: CN-ORH659-73571-95L-00A8 Mouse: SN: 10102UCN	Dell	Windows XP SP3	COTS: PC being used as the Ballot Preparation in a Client/Server configuration setup.
Optiplex GX760: SN: FVMVSK1 Monitor: SN: GROAM00201687 Keyboard: SN: CN-ODJ331-71616-99J-07F1 Mouse: SN: I1905EVQ	Dell	Windows XP SP3	COTS: PC being used as the ERM in a Client/Server configuration setup.
Optiplex GX270 SN: DNC2F51	Dell	Windows XP SP3	COTS: PC being used as the ERM in a Client/Server configuration setup.
Latitude E6400 SN: GD4D6H1 Mouse: SN: X802382-001 PID 56180-523-7959014-0	Dell	Windows XP SP3	COTS: Laptop being used as the ERM in a Client/Server configuration setup.
OptiPlex 760 SN 2HF3CK1 Monitor: SN: CN-OUEH572-46633-683-0V3S Keyboard: SN: CN-ORH659-73541-938-004A Mouse: SN: 01J01F1P	Dell	Windows XP SP3	COTS: PC being used as the ERM in a Client/Server configuration setup.
PowerEdge 600SC X0873024	Dell	Windows 2003 Server	COTS: Server PC in a Client/Server configuration setup.
PowerEdge T410 SN: HS5PVH1 Monitor: SN: 00050480 Keyboard: SN: CN-ODJ331-71616-9CG-	Dell	Windows 2003 Server	COTS: Server PC in a Client/Server configuration setup.

<b>Hardware or Equipment</b>	<b>Manufacturer</b>	<b>Version</b>	<b>Description (identify COTS)</b>
196Y Mouse: D P/N: XN966			
10/100 Dual Speed Hub w/Switch H0GH315000171	D-Link	N/A	COTS: Network Hub for a Closed Network LAN configuration in a Client Server setup
Sandisk Reader Model SDDR-92 SN: 0185431 Model SDDR-91 SN: 377577	ImageMate	None	COTS: Device used to read and write election files to compact flash cards for VAT
(2) OmniDrive USB Professional SN: 790-USB2 SN: 21430-USB	PCMCIA card reader/writer for M100	Setup-CD V2.41 & V3.13	COTS: Drive for reading and writing to SRAM media cards for M100
<b>EMS - Peer to Peer Configuration</b>			
Optiplex GX260 SN: 7D0WL21 Monitor: SN: CN-09M556-64180-2BC-0A45 Keyboard: SN: CN-07N242-38842-2C8-2Q06 Mouse: P/N: 831087-0000	Dell	Windows XP SP3	COTS: PC being used as the Ballot Preparation in a Peer to Peer configuration setup.
Sandisk Reader Model #SDDR-91 no S/N Model #SDDR-92 no S/N	ImageMate	None	COTS: Device used to read and write election files to compact flash cards for VAT
Latitude E6400 SN: 137FMJ1 Mouse: P/N X08-70400 PID 56180-OEM-2678212-6 0423	Dell	Windows XP SP3	COT: Laptop being used as the ERM in a Peer to Peer configuration set up
10/100 Dual Speed Hub w/Switch SN: H0GH314002325	D-Link	N/A	COTS: Network Hub for a Closed Network LAN configuration in a Peer to Peer setup
(3) OmniDrive USB Professional SN: 8814-USB2 SN: 33060-omni SN: 23728-USB	PCMCIA card reader/writer for M100	Setup-CD V2.41 & V3.13	COTS: Drive for reading and writing to SRAM media cards for M100
<b>M650</b>			
M650 Tabulator SN: 2406 8013- Green, Right Oval	ES&S	HW Rev 1.1 FW 2.2.2.0	Central count optical scanner that has color specific optical light and reads right ballot oval.
(2) LQ-590 Printers SN: FSQY093447 SN: FSQY094255	Epson	Model: #P363A	M650 Log and Results report printers (COTS)
(2) Microline 520 Printer SN: 407D4010960 SN: 407D4010894	Okidata	Model: GE5258A	M650 Log and Results report printers (COTS)
Belkin Universal Power Supply SN: 20V06516228WE	Belkin	Model #: None Part #: F6C1500-TW-RK	COTS: M650 Power Supply
Iomega Zip Drive Z250USBPCMBP SN: 1GBS2250K7, 1GBS2641CG	Iomega	N/A	COTS: Central Count M650 Disk Reader/Writer
Iomega Zip Zip M100MB Disks	Iomega	N/A	COTS: Election data and results media
Zip 250MB Disks	FujiFilm	N/A	COTS: Election data and results media
<b>DS200</b>			
ES&S intElect DS200 SN: ES0107370002	ES&S	HW 1.2.0 FW 1.4.3.7	Precinct Count Digital Scanner (Modem removed in ESSUNITY3200)

<b>Hardware or Equipment</b>	<b>Manufacturer</b>	<b>Version</b>	<b>Description (identify COTS)</b>
ES&S intElect DS200 SN: ES0107370025	ES&S	HW 1.2.1 FW 1.4.3.7	Precinct Count Digital Scanner (Modem removed in ESSUNITY3200)
ES&S intElect DS200 SN: ES2093900001	ES&S	HW 1.2.1 FW 1.4.3.7	Precinct Count Digital Scanner (Modem removed in ESSUNITY3200)
ES&S intElect DS200 SN: ES0107380927	ES&S	HW 1.2.1 FW 1.4.3.7	Precinct Count Digital Scanner (Modem removed in ESSUNITY3200)
ES&S intElect DS200 SN: ES0107360007	ES&S	HW Rev 1.2.0 FW 1.4.3.7	Precinct Count Digital Scanner (Modem removed in ESSUNITY3200)
<b>Ballot boxes</b>			
(3) Steel Ballot Box  P/N 76245-10, SN: 1573 P/N 76246, SN: C4243 P/N 76246, SN: TM10177	ES&S	N/A	Precinct Steel Ballot Box for M100 and DS200, No Divterter (SN:1573) Divterter (SN:C4243) Divterter (SN: TM10177)
(1) Plastic Ballot Box (HW Rev.1.2)  Bin P/N 94098 Carrying Case P/N 94099 Emergency Ballot Bin P/N 94325 (P/N is not marked on the Emergency bin)	ES&S	N/A	Precinct Plastic Ballot Boxes for DS200, No Divterter HW 1.2 - Initial product
(4) Plastic Ballot Box (HW Rev.1.3)  Bin P/N 94050 Carrying Case P/N 94051 Emergency Ballot Bin P/N 94325 (P/N is not marked on the Emergency bin)	ES&S	N/A	Precinct Plastic Ballot Boxes for DS200, No Divterter HW 1.3 • Carrying Case: Adhesive & washer/rivets to secure foam in production process Removed the unused switch/bracket • Ballot Bin: Updated locks on the bin Replace a C/B PAR part Metal door instead of plastic door
Plastic blue tote	ES&S	N/A	Plastic blue tote bin for Plastic ballot boxes - 2 locks on wheels
<b>M100</b>			
(3) ES&S Model 100 SN: 205071 SN: 202975 SN: 231531	ES&S	HW Rev 1.3.0 FW 5.4.4.4 Bios v 2.02 OS v 4.22	Precinct Count Optical Scanner (modem removed)
<b>AutoMARK VAT</b>			
AutoMark Voter Assisted Terminal SN: AM0106430376	ES&S	Model A100 HW Rev 1.0 FW 1.3.2907	Accessible paper ballot marking device original release – multiple cable

<b>Hardware or Equipment</b>	<b>Manufacturer</b>	<b>Version</b>	<b>Description (identify COTS)</b>
		OS 5.00.14 PEB 1.65 SBC 1.0	connector and printed circuit boards are mounted in the lower portion of the VAT
AutoMark Voter Assisted Terminal SN: AM0206443384	ES&S	Model A200 HW Rev 1.1 FW 1.3.2907 OS 5.00.14 PEB 1.65 SBC 2.0	Accessible paper ballot marking device. Change: Consolidate PCB, relocate PCB and cables to upper portion for easier maintenance
AutoMark Voter Assisted Terminal SN: AM0206443754	ES&S	Model A200 HW Rev 1.1 FW 1.3.2907 OS: 5.00.19 PEB: 1.70 SBC: 2.5	Accessible paper ballot marking device
AutoMark Voter Assisted Terminal SN: AM0208470815	ES&S	Model A200 HW Rev 1.3.1 FW 1.3.2907 OS: 5.00.19 PEB: 1.70 SBC: 2.5	Accessible paper ballot marking device Change: PEB FW to support Enhanced AutoCast and Double Spit & Wipe (Note: Enhanced Auto Cast is not supported in this version of the VAT FW.)
AutoMark Voter Assisted Terminal SN: AM0208470767	ES&S	Model A200 HW Rev 1.3.1 FW 1.3.2907 OS: 5.00.19 PEB: 1.65 SBC: 2.5	Accessible paper ballot marking device Change: LCD replacement, ROHS board components, change CPU and Flash Chips on the SBC board FW, Win CE OS Bootloader for P30 flash, OS update to support DST and Hash check (Note: Hash check is not supported in this version of the VAT FW.)
Ballot-on-Demand			
COTS - HDN color laser printer			Note: All testing of this product was completed by SysTest Labs; iBeta did not receive this hardware

**Table 9 Voting System Software**

<b>Application</b>	<b>Manufacturer</b>	<b>Version</b>	<b>Description (identify COTS)</b>
Election Management Software			
Election Data Manager	ES&S	7.8.1.0	EMS software for election definition and ballot preparation for M650, DS200, and M100
ES&S Ballot Image Manager (ESSIM) with Ballot On Demand (BOD)	ES&S	7.7.1.0	Unity election management system desktop publishing tool to layout and format paper ballots  BOD is an optional operating mode in ESSIM used to print election quality ES&S paper ballots on a COTS OKI 9600 HDN color laser printer.
Audit Manager (AM)	ES&S	7.5.2.0	A Unity election management system audit logging software application including security and user tracking for the Election Data

<b>Application</b>	<b>Manufacturer</b>	<b>Version</b>	<b>Description (identify COTS)</b>
Manager and Ballot Image Manager			
Hardware Programming Manager (HPM)	ES&S	5.7.3.0	A Unity election management system software application to import, format, and convert an election file and create election definitions for ballot scanning equipment
AIMS (Automark information Management System)  Note: VAT Preview is configured within the AIMS application. When installing VAT Preview, the AIMS media will be used.	ES&S AutoMARK	1.3.257	A windows-based election management system software application to define election parameters for the VAT, including functionality to import election definition files produced by the Unity EMS and create VAT flash memory cards
Voter Assist Terminal (VAT)	ES&S AutoMARK	1.3.2907	A software application to assist multilingual voters and voters with visual, aural or dexterity disabilities to vote a paper ballots in a private manner
Election Reporting Manager (ERM)	ES&S	7.5.7.0	A Unity central count software application to compile and report election results. v.7.5.5.0 includes a fix to ESSUnity3200 v.7.5.4.0 for discrepancy #104. It is tested to VVSG 2005
Log Monitor	ES&S	1.0.0.0	A software application that checks the status of the Windows Event Log feature and closes all ES&S applications if the Event Log feature is disabled or not configured properly.
Microsoft Windows XP	Microsoft	Service Pack 3	COTS personal computer operating system.
Acrobat Standard	Adobe	9	COTS software used with ESSIM to create ballot files for printing.
RM/COBOL	Liant	11.01	COTS interpreter software used in HPM & ERM
Adobe Type Manager	Adobe	4.1	COTS software used with ESSIM to create ballot files for printing
AVG Anti-Virus	AVG	9.0 Business Edition	COTS Anti Virus protection for PCs and Servers
Microsoft Windows Server 2003	Microsoft	Service Pack 2	COTS server operating system
Adobe Type Basic	Adobe		COTS software used with ESSIM to create ballot files for printing
Heise CTUPDATE	Heise / Microsoft		COTS software used to collect all Microsoft update to install on PC
OmniDrive USB	OmniDrive	2.4.1	COTS software used to generate media on an OmniDrive
<b>Polling Place</b>			
intElect DS200	ES&S	1.4.3.7	Precinct count digital scanner paper ballot tabulator including a 12-inch touch screen display providing voter feedback and poll worker messaging. DS200 scanner reads marks on both one- and two-sided ballots. Administrators can request custom ballot acceptance criteria, which

<b>Application</b>	<b>Manufacturer</b>	<b>Version</b>	<b>Description (identify COTS)</b>
			ES&S programs onto the scanner's election definition.
M100	ES&S	5.4.4.4	Precinct-based, voter-activated paper ballot counter and vote tabulator. The M100 simultaneously read both sides of the ballot, and record the voter selections. The M100 may also be used as a central tabulator but functionality is no different than Precinct Count tabulator. Optional connection of a COTS results printer which overrides operation of the M100 printer when connected
Central Count			
Model 650 (M650)	ES&S	2.2.2.0	Central count high-speed optical scanner paper ballot tabulator. The scanner checks the pre-printed codes along the ballot edge to determine each ballot's precinct, split and type. The M650 prints results reports to an external printer and saves results to a zip disk.

**Table 10 Voting System Technical Data Package Documents**

<b>Title</b>	<b>Version</b>	<b>Date</b>	<b>Author (Organization.)</b>
<b>Unity 3.2.1.0</b>			
AutoMARK Information Management System Election Official's Guide	20	3/11/2010	ESS
AutoMARK VAT Firmware and Hardware Installation Instructions	15	9/28/2009	ESS
ES&S Ballot Production Handbook Version 1.0.0.0	None	7/17/2007	ESS
Installation of the E-Bin Ballot Diverter Extensions for the DS200 Ballot Box	None	No date	ESS
Voting System Overview Unity v. 3.2.1.0	16	9/15/2010	ESS
2002 VSS Supported Functionality Declaration	4	8/11/2009	ESS
System Limitations Unity v. 3.2.1.0	8	3/9/2010	ESS
Ballot Data File Specification Unity Version 4.0.0.0	None	6/12/2007	ESS
ES&S DS200 System Maintenance Manual Hardware Version 1.2.1			
Firmware Version 1.4.3.6	None	9/17/2010	ESS
ES&S M100 System Maintenance Manual Firmware Version 5.4.4.3			
Hardware Version 1.3	None	8/20/2010	ESS
ES&S Model 650 System Maintenance Manual Firmware Version 2.2.2.0			
Hardware Version 1.1 and 1.2	None	8/17/2010	ESS
ES&S Audit Manager System Operations Procedures Version Release 7.5.2.0	None	8/13/2009	ESS
Audit Manager Checklist Election Day Training Manual Unity Version 3.2.1.0	None	Jan-10	ESS
ES&S DS200 System Operations Procedures Hardware Version 1.2.1			
Firmware Version 1.4.3.6	None	9/17/2010	ESS
ES&S Election Data Manager System Operations Procedures Version Release 7.8.1.0			
Election Data Manager (EDM) Checklist Election Day Training Manual Unity Version 3.2.1.0	None	Jan-10	ESS
ES&S Election Reporting Manager System Operations Procedures Version Release 7.5.7.0			
ES&S Image Manager System Operations Procedures Version Release 7.7.1.0	None	9/3/2010	ESS
ESS Image Manager (ESSIM) Checklist Election Day Training Manual Unity Version 3.2.1.0	None	6/7/2010	ESS

Title	Version	Date	Author (Organization)
ES&S Ballot On Demand Printer Setup and Printing Procedures Version Release 7.7.1.0 Okidata part number 58273508	None	6/7/2010	ESS
ES&S Hardware Programming Manager System Operations Procedures Version Release 5.7.3.0	None	9/3/2010	ESS
Hardware Programming Manager (HPM) Checklist Election Day Training Manual Unity Version 3.2.1.0	None	Jan-10	ESS
ES&S LogMonitor System Operations Procedures LogMonitor 1.0.0.0	None	8/28/2009	ESS
ES&S Model 100 System Operations Procedures Firmware Version 5.4.4.3 Hardware revision 1.3	None	8/27/2010	ESS
ES&S Model 650 System Operations Procedures Firmware Version 2.2.2.0 Hardware Version 1.1 and 1.2	None	8/17/2010	ESS
General County, USA M100 - DS200 - ESS AutoMARK - RTAL - M650 Phased Approach Integrated Schedule (Preliminary Timeline)	None	No date	ESS
Installing Adobe COTS Products	None	5/28/2008	ESS
OmniDrive USB/USB2 Installation Guide USB2 Driver V3.11 PC Card Manager V. 2.01 Document Version 1.0	1	5/20/2008	ESS
RM/COBOL® Installation Guide Version 11.01	1.1	5/20/2008	ESS
ES&S System Security Specification Version Release 3.2.1.0	None	4/16/2010	ESS
Jurisdiction Security Procedures Election Systems and Software Version 1.0.0.1	None	3/12/2010	ESS
DS200 Validation Guide	1	1/11/2010	ESS
DS200 Validation – File Listing	1	1/11/2010	ESS
Model 650 Validation Guide	1	1/11/2010	ESS
Model 650 Validation Guide – File Listing	1	1/11/2010	ESS
AutoMARK Validation Guide	1	1/11/2010	ESS
AutoMARK Validation Guide - File Listing	1	1/11/2010	ESS
Unity Workstation Validation Guide	1	10/30/2009	ESS
Unity Workstation Validation – EDM File Listing Unity 3.0.1.1 EAC	1	10/30/2009	ESS
Unity Workstation Validation – Audit Manager File Listing Unity 3.0.1.1 EAC	1	10/30/2009	ESS
Unity Workstation Validation – ES&S Ballot Image Manager File Listing Unity 3.0.1.1 EAC	1	10/30/2009	ESS
Unity Workstation Validation – Hardware Programming Manager File Listing Unity 3.0.1.1 EAC	1	10/30/2009	ESS
Unity Workstation Validation – AIMS File Listing Unity 3.0.1.1 EAC	1	10/30/2009	ESS
Unity Workstation Validation – VAT Preview File Listing Unity 3.0.1.1 EAC	1	10/30/2009	ESS
Unity Workstation Validation – ERM File Listing Unity 3.0.1.1 EAC	1	10/30/2009	ESS
Model 100 Validation Guide	7	11/23/2009	ESS
Deployment Media Validation Guide	1	9/28/2009	ESS
Hardening Procedures Election Management System PC Unity 3.2.1.0	5	9/2/2010	ESS
Unity 3.2.1.0 ES&S Software Installation Order	1	9/25/2009	ESS
Audit Manager Training Manual Version 7.5.x	None	7/31/2009	ESS
AutoMARK Election Day Checklist Version Number 1.3.x	None	7/31/2009	ESS
AutoMARK Pre-Election Day Checklist Version Number 1.3.x	None	7/31/2009	ESS
DS200 Precinct Ballot Scanner Election Day Training Manual Version Number 1.4.x	None	6/7/2010	ESS
DS200 Precinct Ballot Scanner Pre-Election Day Training Manual Version Number 1.4.x	None	6/7/2010	ESS
Election Data Manager Training Manual Version Number 7.8.x	None	7/31/2009	ESS
Election Reporting Manager Pre-Election Day Training Manual Version Number 7.5.x	None	6/7/2010	ESS
ESSIM Training Manual Version Number 7.7.x	None	7/31/2009	ESS
Election Results Export (EXP) Election Day Checklist Version Number 3.0.x	None	7/31/2009	ESS
Hardware Program Manager Training Manual Version Number 5.7.x	None	7/31/2009	ESS
Model 100 Election Day Checklist Version Number 5.4.x	None	6/7/2010	ESS
Model 100 Pre-Election Day Checklist Version Number 5.4.x	None	6/7/2010	ESS
Model 650 Election Day Checklist Version Number 2.2.x	None	7/31/2009	ESS

Title	Version	Date	Author (Organization)
Model 650 Pre-Election Day Checklist Version Number 2.2.x	None	7/31/2009	ESS
ES&S Personnel Deployment and Training Recommendations Unity v. 3.2.1.0	3	1/11/2010	ESS

**Table 11 Testing Software, Hardware and Materials**

Software, Hardware or Material	Description	Description of use in testing
DS200		
Delkin Thumb Drives: 512MB 2GB, 4GB & 8GB	Storage media for the DS200	COTS: Media for installing election definition, recording and reporting votes and audit logs
SanDisk Thumb Drives: 1GB, 2GB	Storage media for the DS200	COTS: Media for installing election definition, recording and reporting votes and audit logs
M650		
Iomega Zip Disk 100MB	Storage media for the M650	COTS: Media with election definition and results totals for M650
ES&S M650 Output Tray	Central Count Ballot Output Tray	Central Count Ballot Output Tray for ballots scanned
M100		
Vikant Corporation PCMCIA SRAM Card 512k, with a Panasonic 3V Battery BR2325 manufacture P/N: SJA-512KJC	Storage media for M100 - requires a 3V battery for operation	COTS: Media for installing election definition, recording and reporting votes and audit logs
Centon 512k & 4meg SRAM Card, with a 3V lithium battery BR2325 manufacture P/N: PCMCIA003	Storage media for M100	COTS: Media for installing election definition, recording and reporting votes and audit logs
AutoMARK VAT		
SanDisk Compact Flash Memory Card 256MB	Storage media for the VAT	COTS: Media for installing election definition on the VAT
AutoMark Inkjet Print Cartridge	Print cartridge for VAT	Replacement ink cartridges for VAT
Foot Pedal	Alternative vote input device for VAT	Allows the user to alternatively cast votes.
AutoMark Programming Cable	Cable use for AutoMARK firmware Installs	Used to install firmware on the AutoMARK
Headphones	Alternative vote listening device for VAT	Allows the voter to listen to audio instructions and contests on the AutoMARK VAT
Test Material		
Paper rolls	Paper, Thermal Printer	COTS: DS200 and M100 reports
Paper Ballots	Paper Ballots - 11", 14", 17" & 19", 3 and 4 ovals per inch	Supplied by ES&S: Miscellaneous ballots for VAT, DS200, M100, M650 with preprinted election content, and blank ballot stock for VAT audit log
Paper	81/2 x 11 Printer paper  M650 Continuous feed paper	COTS: for reports from AM, EDM, ESSIM, HPM, ERM reports  COTS: for Central count (M650) audit log and reports
HP LaserJet Printer 4050N SN: 600004	Report Printer	COTS: Used for printing reports from EDM, HPM, ERM, and ESSIM for the Peer to Peer setup.
Ballot Marker Pens	Marking Device	COTS: VL Ballot Pen to mark paper

<b>Software, Hardware or Material</b>	<b>Description</b>	<b>Description of use in testing</b>
OKI Printer B410dn SN: AF92017190A0	Network Printer	COTS: Used for printing reports from PCs connected to Hubs for Server setup.
Ethernet Cables	Cables for the LAN	COTS: Transfer election management data among workstations and/or servers on the EMS LAN
<b>Test Management and Tools</b>		
Multiple desktop and laptop PCs	A variety of PCs running Microsoft operating systems	Supplied by iBeta: Preparation, management and recording of test plans, test cases, reviews and results
Repository servers	Separate servers for storage of test documents and source code, running industry standards operating systems, security and back up utilities	Supplied by iBeta: Documents are maintained on a secure network server. Source code is maintained on a separate data disk on a restricted server
Microsoft Office 2003 & 2007	Excel and Word software and document templates	Supplied by iBeta: The software used to create and record test plans, test cases, reviews and results
SharePoint 2003	TDP and test documentation repository	Supplied by iBeta: TDP and test documentation repository and configuration management tool
Other standard business application software	Internet browsers, PDF viewers email	Supplied by iBeta: Industry standard tools to support testing, business and project implementation
RSM v.6.92 (M Squared Technologies)	C, C++, Java & C# static analysis tool	Supplied by iBeta: identify line counts and cyclomatic complexity
Beyond Compare 2 v.2.4.3 (Scooter Software)	Comparison utility	Supplied by iBeta: used to compare file/folder differences
WinDiff 5.1 (Microsoft)	Comparison utility	Supplied by iBeta: used to compare file/folder differences
Hash.exe v.7.08.10.07.12 (Maresware)	Hash creation utility	Supplied by iBeta: used to generate hash signatures for Trusted Builds
Symantec Ghost v. 11	Image capture tool	Supplied by iBeta: used to capture and test environments.
SLAX LIVE W/ SHA1DEEP v.5.1.8	Hash creation tool	Supplied by iBeta: used to generate hash signatures for the M100
Center 325 Mini Sound Level Meter	IEC 651 Type 2 handheld sound level meter	Supplied by iBeta: Measure decibel level
Visual Studio 2008 v. 9.0.21022.8 (Microsoft)	Build and source code review Integrated Development Environment	Supplied by iBeta: View source code review
Bart PE 3.1.10a	Ghost utility	Supplied by iBeta: used with Ghost process
Knoppix 5.1.0	Hash creation utility	Supplied by iBeta: used to generate hash signatures
Nessus v.4.1	Penetration testing	Supplied by iBeta: used to perform penetration testing
Teltone TLS-5A-02	PBX testing	Supplied by iBeta: used in PBX testing
US Robotics 56K Faxmodem	Modem testing	Supplied by iBeta: used when testing modem connectivity (serial modem)
Killdisk v.4.1	PC clear utility	Supplied by iBeta: used to wipe clean PCs and servers prior to testing

## **4 Voting System Overview**

The ES&S Unity 3.2.1.0 is a paper-based voting system that incorporates the Model 100 Precinct Scanner plus the hardware, firmware and software previously certified in the **ESSUNITY3200** voting system. It consists of the election management software applications: Election Data Manager (EDM), ES&S Ballot Image Manager (ESSIM), Hardware Programming Manager (HPM), AutoMARK Information Management System (AIMS); the audit software, Audit Manager and LogMonitor Service; and the Election Reporting Manager (ERM) central count reporting software. Paper ballots can be printed by Ballot-on-Demand COTs printer in addition to providing ballots to commercials printers for printing. The voting system includes the DS200 and M100 precinct optical scanner hardware and firmware, the AutoMARK Voter Assist Terminal A100, AutoMARK Voter Assist Terminal Model A200 precinct ballot marker hardware and firmware and the Model 650 central count hardware and firmware. The Unity 3.2.1.0 voting system election management system may be configured as individual stand alone platforms, platforms connected through peer-to-peer file sharing or platforms setup in a Windows 2003 Server local area network.

### **4.1 *Election Management System- Pre Voting Capabilities***

The Unity 3.2.1.0 election management system pre-vote functions are performed by the six software applications installed on a stand-alone PC or multiple PCs in either a peer-to-peer or Windows 2003 Server configuration.

#### **4.1.1 *Election Data Manager (EDM)***

The Election Data Manager functionality includes:

- Definition of election databases for the M650, M100 and DS200 paper ballot scanners and VAT paper ballot markers;
- Creation and edit of closed, open and pick-a-party primaries and general elections with office, candidate election, and absentee preferences;
- Set up of early, Election Day and absentee voting;
- Creation and edit of new elections from existing files;
- Creation and edit of ballot sets, rotations, groupings and straight party;
- Creation and edit of parties, candidates, referendum, recall questions, and write-in targets;
- Creation, edit and assignment of precincts and polling places;
- Creation, edit and generation of ballot styles;
- Merging preferences;
- Use of the Import Wizard to import lists of parties, language, precincts, county, district typed, district names, district relations, office headings, office relations, candidates, and polling places;
- Addition and edit of language files;
- Select and generate statistical counters;
- Display, print and export of EDM reports, including: Master Precinct Report, District Names, District Relations, District Relations by Precinct, Master Office, Party, Office Headings, Precincts this Election, Offices this Election, Office Relations, Candidates this Election -in party order sorted by last name, Offices and Candidates this election Ballot Styles in Ballot Style Order, Ballot Styles in Precinct Order, Ballot Galley Report (Precinct/Office/Candidate), Candidate Rotations by Office, and Standard Rotation;
- Generates the interface file(.iff) and ballot set collection file (.bsc) to create the ballot data file (.bdf); and
- Back up of election files.

#### **4.1.2 ES&S Ballot Image Manager (ESSIM)**

The ES&S Image Manage (ESSIM) is a desktop publishing tool to design and publish ES&S paper ballots for the Unity 3.2.1.0 DS200 and M100 precinct scanners, and the M650 central count scanner. ESSIM is used to:

- Import the ballot data file(.bdf) from EDM;
- Create and edit ballot formats for ES&S ballot services or a printer to print official ballots;
- Create and edit style sheets for ballot elements corresponding to EDM election data (offices, parties, candidates, etc.);
- Create and edit text frames to place instructional text on a ballot;
- Create and edit graphic frames to place images on a ballot;
- Create and edit production frames to place variable information (precinct or style identifiers) on a ballot;
- Reuse previously created ballot formats;
- Use layouts created with the program to print extra Election Day ballots with Ballot on Demand;
- Reads and convert the information contained in an EDM election database into finished ballot layouts;
- Generation of the interface file (ifc);
- Generate Ballot Validation and Ballot Style Reports to validate election data properly fits the ballot and is properly positioned; and
- Package elections for back up, transfer to other computers or send to ES&S as requested for election support.

#### **4.1.3 Hardware Programming Manager (HPM)**

Hardware Programming Manager (HPM) is used to convert the election file for use with Election Reporting Manager (ERM) and for create election parameters and loading them to the memory device for the DS200, M100 or M650.

- Create and edit the election shell for importation of the interface file (.ifc);
- Create and edit access control for HPM, the M100 and DS200;
- Set and edit jurisdiction tabulator controls for selection of equipment and tape/report printing sequence and "vote for" information;
- Set and edit election specification tabulator controls for handling of blank, cross-voted, write-ins; unreadable marks, absentee ballots and report printing;
- Set and edit certification tabulator controls for text to appear on reports and tapes;
- Write elections to zip disk, PCMCIA card, and USB memory storage devices for the M650, M100 and DS200;and
- Update the election for use by AutoMARK Information Management System (AIMS) and the Election Reporting Manager (ERM).

HPM may also be used for coding an election, if necessary. HPM permits importation, formatting, and conversion of the election file, definition of districts, election contests and candidates, election definitions for ballot scanning equipment.

#### **4.1.4 AutoMARK Information Management System (AIMS)**

The AutoMARK Information Management System includes the AIMS application software installed on a COTS PC. It was originally developed by Automark Technical Services, LLC (ATS) and acquired by ES&S. ES&S has assumed responsibility for the product. The AIMS application manages information required by the AutoMARK Voter Assist Terminal (VAT) for an election, including:

- Importation of HPM election files and a corresponding printed optical scan ballot;
- Optional manual entry of election data;

- Edit of stored election multilingual text information for proper pronunciation of synthesized speech messages;
- Storing of recorded multilingual voice messages in WAV format;
- Writing of the election database to a compact flash memory card (FMC) in order to provide ballot content information to the VAT;
- Review ballot set-up and preview on-screen ballot display;
- Performs no ballot counting or vote counting/reporting functions;
- Logging of changes to the election database in the AIMS audit log; and
- Backing up (archive) of the election database.

#### **4.1.5    *Audit Manager (AM)***

EDM and Image Manager use Audit Manager to store detailed logs of the actions performed in both programs. Audit Manager:

- Prints or displays audit listings;
- Listings include date and time stamps;
- Listings can be exported;
- Displays logs in cascade, vertical and horizontal views; and
- Archives logs.

#### **4.1.6    *LogMonitor***

The LogMonitor is an application that checks the status of the Windows Event Log. It does not permit the ES&S applications to run if the Windows Event Log is disabled, improperly configured or stops operating.

## **4.2    *Polling Place- Voting Capabilities***

The Unity 3.2.1.0 polling place voting functionality is performed by the intlElect DS200 Precinct Scanner, the Model 100 precinct scanner, and the AutoMARK Voter Assist Terminal.

#### **4.2.1    *Model 100***



The ES&S Model 100 is a precinct-based, voter-activated paper ballot counter and vote tabulator. The M100:

- Is designed with a real time audit log of all transactions;
- Can print paper reports from the tabulator's internal, thermal printer or by an external printer connected to the tabulator;
- Uses a removable PCMCIA card to transfer tabulator results to Election Reporting Manager after the polls close;
- Permits opening, closing and reopening of the polls;
- Automatically prints a Zero report when the polls open;
- Uses advanced Intelligent Mark Recognition (IMR) visible light scanning technology;
- Accepts ballots inserted in any orientation and has optical scanners that read both sides of the ballot.
- Has the ability to alert voters of blank, undervoted and overvoted ballots, which can be returned to the voter to provide them the opportunity to revise and recast the ballot;
- Does not store any ballot data, all ballot and election data are stored on a PCMCIA card locked in place on the front of the scanner;
- Has a public counter that displays the number of ballots cast;
- Back-up battery power obtains its charge automatically from the system power supply;
- Permits programming of separate election groups for the procedural processing and storage of provisional ballots separately from Election Day totals for inclusion, after determination of voter validity; and
- Supports Early Voting.

#### **4.2.2 *intlElect DS200 Precinct Ballot Scanner***

The intlElect DS200 is a jurisdiction-wide election tabulation system. DS200 scanners were certified in **ESSUNITY3200**. Cosmetic and functional changes submitted to the firmware in Unity 3.2.1.0 did not impact the system overview description except to increase the number of precincts supported.



The intlElect DS200 scanners:

- Process single or dual-sided paper ballots for up to 18 Election Day precincts and 1639 Early Voting precincts;

- Permit programming of separate election groups for the procedural processing and storage of provisional ballots separately from Election Day totals for inclusion, after determination of voter validity;
- Supports Early Voting;
- Permit opening, closing and reopening of the polls;
- Automatically prints a Zero report when the polls open;
- Can be configured to automatically print one or more reports (Status, Race Results, Certification or Audit Log)
- Have a public counter that displays the number of ballots cast;
- Store paper ballots in attached ballot storage bins (key locked ballot boxes);
- Do not store any ballot data; all ballot data, election totals and optional ballot images are stored on an external USB flash drive which can be transported to a central count location;
- Prevents access to the USB election flash drive via a key locked compartment;
- Print reports including: Election Startup, Poll Closing, Diagnostic, Initial State, Audit Log, Zero and Certification;
- Audit logging and reporting;
- Operates on standard or two hour back-up battery power.

#### **4.2.3 AutoMARK Voter Assist Terminal (VAT)**

The AutoMARK VAT is an automated voter assistive paper ballot marking device. It was originally developed by Automark Technical Services, LLC (ATS) and acquired by ES&S. ES&S has assumed responsibility for the product. Four configurations of the VAT were certified in **ESSUNITY3200**. No changes have occurred in Unity 3.2.1.0. A description of the five configurations and their differences is found in [Section 3.1 Submitted Voting System Identification](#).



The VAT device assists voters with visual, language and manual dexterity challenges. It only displays ballot for marking on paper. Temporary memory only retains votes until the printing operation is complete. VSS requirements for a DRE are applicable for ballot display and voter selection functions, only. The VAT is exempt from vote storage and reporting function requirements.

The VAT:

- Incorporates a touch screen monitor, tactile input buttons, connections for assistive input devices, audio output and a ballot marking printer;
- Password protects the System Maintenance Menu for setting date/time and loading firmware;
- Permits installation of an AIMS election database on a compact flash memory card;

- Provides a test mode for performance of set-up, reporting and maintenance functions;
- Provides audio, printing, screen and button readiness tests and verification of the ballot definition;
- Draws a preprinted blank ballot from the voter input tray and scans a preprinted bar code on the ballot to determine the form of ballot inserted;
- Presents the voter with the options to make a language selection for either an audio or visual ballot;
- Presents the voter with controls to adjust the display contrast/size, volume, speed for synthesized speech and repeat audio output;
- Present the ballot as a series of menu-driven voting choices on a color screen;
- Permits vote selection inputs via a touch screen or assistive switch-based devices (foot paddles);
- Accumulates the voter's choices in an internal memory until the voter has completed the selection process;
- Provides a summary of the voter's choices for review and confirmation;
- Marks and prints the paper ballot following voter confirmation of the summary;
- Accommodates insertion of the ballot in any orientation;
- Prints single and double-sided ballots;
- Returns the ballot to the voter after printing is completed;
- Clears its internal memory so that the paper ballot is the only lasting record of voter selections;
- Prevents access to the compact flash memory card via a key locked compartment;
- Operates on standard or back-up battery power; and
- Provides a date/time stamped audit log of ballot marking operations that can be viewed or printed.

### **4.3 Central Count Scanner- Post Voting Capabilities**

The central count scanner functions are performed by the Model 650 Central Ballot Scanner.

#### **4.3.1 Model 650 Central Ballot Scanner (M650)**

The Model 650 Central Ballot Scanner is a high-speed, computerized, paper ballot, optical mark reader.



The M650 scanner:

- Options include a left and right ballot oval read and red and green light optical read;
- Loads and tests election definitions and readiness for Election Day tasks;
- Checks the pre-printed codes along the ballot edge to determine each ballot's precinct, split and type;

- Reads voter choices for candidates or issues in a fraction of a second for each ballot;
- Checks for ballot irregularities, stops and provides the operator instructions for handling the ballot;
- Tabulates votes in each race and tracks the race count and total ballots by precinct;
- Permits separate scanning for Election Day and Absentee ballots;
- Permits sorting of over-voted, blank and write-in ballots;
- Tracks absentee results by a user determined method defined in the election definition;
- Clearing of vote counts to permit rescanning for accidental user counting errors;
- Generates printed reports on-demand to provide up-to-the-minute totals by precinct, city, or by county;
- Provides report options for inclusion of over and under-votes, totals per race, ranking of candidate by votes received, certification messages and write-ins;
- Provides a time/date stamped audit log of scanner activities on a separate printer.
- Saves election results to a zip disk in order to make a permanent record of the election, transfer to ERM or to use as backup data;
- Permits adding of vote totals from a zip disk into the scanner; and
- Network card can be removed to disable networking capabilities (Networking is excluded from testing in Unity 3.2.1.0).

## **4.4 *Election Management System- Post Voting Capabilities***

The post vote consolidation and reporting functions are performed by the Election Reporting Manager.

### **4.4.1 *Election Reporting Manager***

Election Reporting Manager (ERM) is ES&S's election results reporting program. ERM is designed to display updated election totals on a monitor as election data is consolidated. ERM:

- Supports configuration of uses and user permissions to limit access to specific functions;
- Warns the user when votes are present in the election database at startup;
- Supports creation of the Results Database for an election;
- Supports creation and definition of Groups;
- Only supports importation of election results from the M100 on PCMCIA cards, M650 on zip disks and DS200 on USB memory drives in Unity 3.2.1.0;
- Supports manual entry of hand counted election results;
- Supports close out of Precincts with no ballots cast;
- Generates paper and electronic reports: including ; Precinct, Precinct Group Detail, Election Summary, election Summary with Group Detail, Canvas (Numbered Key, Statistics, Numbered Key Districts only, Numbered Key Districts Turnout only, Name heading, District Totals, Block Style, Jurisdiction, Local Office, Precincts Counted Precincts Completed Listing, Precincts Process Listing), and System Log;
- Supports temporary suppression and subsequent release of precinct results for unique circumstances that may require investigation prior to release of results to prevent counting errors or vote total altering problems;
- Supports merging of election results from multiple ERM with files transferred on 3.5 inch disk, other appropriate memory devices, or in a peer-to-peer or client/server local area;
- Support creation of state specific transfer and web files;
- The hardened ERM platform does not support receipt of election results from the M100 or DS200 via the public telephone or on an internal LAN from the M650 in Unity 3.2.1.0 (no testing was performed for network transmission of results).
- Was not submitted for use with the iVotronic in Unity 3.2.1.0 (no testing was performed with these tabulators).

## 5 Certification Review and Test Results

The results and evaluations of the PCA and FCA reviews tests are identified below. Detailed data regarding the Acceptance/Rejection criteria, reviews and tests are found in the appendices.

- [Appendix A](#) identifies all certification test requirements traced to specific Test Cases
- [Appendix B](#) identified the PCA Source Code Review Acceptance/Rejection criteria
- [Appendix C](#) identifies the PCA TDP Document Review Acceptance/Rejection criteria
- [Appendix D](#) identifies all FCA Testing Acceptance/Rejection criteria
- [Appendix E](#) identifies the PCA and FCA Discrepancies reported during review and testing

### 5.1 PCA Source Code Review

The PCA Source Code Review addresses the standard code review called out in VSS vol. 1 sect. 4.2 and vol. 2 sect. 5.4. Unique source code reviews that were conducted for specific Functional and Security requirements are found in [Sections 5.3](#) and [5.5](#).

- The M100 source code review was performed by SysTest in the Unity 4.0.0.0 test effort. iBeta performed a 3% Source Code Review and provided a recommendation to the EAC regarding reuse of the SysTest code review for Unity 3.2.1.0. The 3% source code review was conducted using iBeta's standard PCA Source Code Review Procedure. The detailed process for this review is found in the [Appendix H Amended Test Plan](#) (see section 2.1.3.1 Documentation of the 3% Source Code Review Process). Any changed or new code submitted by ES&S for Unity 3.2.1.0 was 100% reviewed by iBeta to the VSS 2002 using iBeta's standard PCA Source Code Review Procedure.
- Source code that remained unchanged from the **ESSUNITY3200** certification did not require any additional review or a new Trusted Build. The builds of the unchanged applications were moved into the Unity 3.2.1.0 project from the ESSUNITY3200 escrow. iBeta conducted a 100% review of source code changes that were submitted by ES&S in Unity 3.2.1.0. All changes made to the ESSUNITY3200 certified code were reviewed to the VVSG 2005.
- During receipt and check in of the Unity 3.2.1.0 source code delivered by ES&S, iBeta observed if the source code version control was consistent with the ES&S configuration management practices.

The Unity 3.2.1.0 Source Code Review Results are listed below. The data supporting these reviews are found in [Appendix B](#).

#### 5.1.1 M100 C Source Code Review Results

M100 consists of a C component. The reviewed Unity 4.0.0.0 source code was delivered to iBeta by SysTest. A 3% sampling of 25 functions was selected. Each of these functions was 100% reviewed for conformance to the VSS 2002. There were no instances of non-conformance reported and the SysTest code review was recommended for reuse. This became the baseline Unity 3.2.1.0 code delivery.

ES&S submitted changes to this baseline. A total of 63 changed functions were reviewed. Each of the changed functions was 100% reviewed for conformance to the VSS 2002. One instance of non-conformance was reported to ES&S. ES&S submitted a fix and it was validated resolved. The discrepancy was comment related. There were no discrepancies against any of the software related VSS 2002 requirements. The file function line count results identified no files or functions exceeded 240 eLOCs, 8.63% were between 60 and 120 lines, 1.35% were between 120 and 240 lines, the remaining 90.02% were less than 60 lines. The source code was found to meet the requirements of the VSS 2002. The data supporting this review are found in [Appendix B](#).

### **5.1.2 DS200 C/C++,Scanner-c8051 C and MYDLL C Source Code Review Results**

DS200 consists of C/C++ components. The **ESSUNITY3200** baseline was modified during the Unity 3.2.1.0 test effort. A total of 651 functions were changed. Each of the changed functions was 100% reviewed for conformance to the VVSG 2005. There were 42 instances of non-conformance reported to ES&S. ES&S submitted fixes and they were validated as resolved. All source code discrepancies were comment related. None of the discrepancies were against any of the software related VVSG 2005 requirements. The file function line count results identified no files or functions exceeded 240 eLOCs, 3.47% were between 60 and 120 lines, .23% were between 120 and 240 lines, the remaining 96.30% were less than 60 lines. The source code was found to meet the requirements of the VVSG 2005. The data supporting this review are found in [Appendix B](#).

### **5.1.3 VAT VB. Net Source Code Review Results**

VAT consists of a VB.Net component. The **ESSUNITY3200** baseline was modified during the Unity 3.2.1.0 test effort. A total of 5 functions were changed. Each of the changed functions was 100% reviewed for conformance to the VVSG 2005. One instance of non-conformance was reported to ES&S. ES&S submitted a fix and it was validated resolved. The discrepancy was comment related. The discrepancy was not against any of the software related VVSG 2005 requirements. The file function line count results identified no files or functions exceeded 240 eLOCs, 4.59% were between 60 and 120 lines, 1.60% were between 120 and 240 lines, the remaining 93.72% were less than 60 lines. The source code was found to meet the requirements of the VVSG 2005. The data supporting this review are found in [Appendix B](#).

### **5.1.4 HPM and ERM COBOL Source Code Review Results**

HPM consists of a COBOL component. The **ESSUNITY3200** baseline was modified during the Unity 3.2.1.0 test effort. A total of 15 functions were changed. Each of the changed functions was 100% reviewed for conformance to the VVSG 2005. There were no instances of non-conformance reported against HPM. The file function line count results identified HPM had no files or functions exceeded 240 eLOCs, 11.11% were between 60 and 120 lines, 0.00% were between 120 and 240 lines, the remaining 88.89% were less than 60 lines. The source code was found to meet the requirements of the VVSG 2005. The data supporting this review are found in Appendix B.

ERM consists of a COBOL component. The **ESSUNITY3200** baseline was modified during the Unity 3.2.1.0 test effort. A total of 52 functions were changed. Each of the changed functions was 100% reviewed for conformance to the VVSG 2005. Thirteen instances of non-conformance were reported to ES&S against ERM. ES&S submitted fixes and these were validated as resolved. These discrepancies were comment related. These discrepancies were not against any of the software related VVSG 2005 requirements. The file function line count results identified ERM had no files or functions exceeded 240 eLOCs, 0.00% were between 60 and 120 lines, 0.00% were between 120 and 240 lines, the remaining 100% were less than 60 lines. The source code was found to meet the requirements of the VVSG 2005. The data supporting this review are found in [Appendix B](#).

### **5.1.5 AIMS Source Code Review Results**

There is no source code difference in version 1.3.157 and 1.3.257, but there is a difference in Build package "AIMS ESS Installation.ism" multi-user environment.

The data supporting this review are found in [Appendix B](#).

## **5.2 PCA TDP Document Review**

The *Unity 3.2.10 PCA TDP Documentation Review* included an initial review of the M100, new or updated documentation to confirm that the content required in the VSS 2002 vol.2 section 2 was present in the applicable document(s). If the required content was present the review was marked "Accept." If the content was not present the review was marked "Reject". Issues noted as "Reject" were logged into the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#) as "Document Discrepancies". The discrepancy number was

cross referenced in the PCA TDP Document Review form. ES&S addressed the rejected items and resubmitted updated versions of the documents. Upon review and acceptance of the revised document the PCA TDP Document Review was updated to "Accept", the verification of the correction was noted in the discrepancy report and marked closed.

Documents previously reviewed in the **ESSUNITY3200** certification test effort were rebranded by ES&S to reflect Unity 3.2.1.0 voting system. These rebranded documents were resubmitted. iBeta compared the resubmitted documents to the certified **ESSUNITY3200** version to confirm if any changes impacted the requirements of VVSG 2005 vol.2 section 2. (Note: This section is identical in the VSS 2002 and VVSG 2005.) It was found that the document changes did not impact these requirements. Verification for reuse of the **ESSUNITY3200** was recorded in the PCA Document Review form.

Quality Assurance reviewed the ES&S M100 and changes to the **ESSUNITY3200** TDP documents against the Vol. 2 Sect. 2 requirements of the VSS 2002 and VVSG 2005. Any instance of inconsistency in the version control of materials delivered by ES&S was reported in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#) as an informational issue.

Additionally, a Quality Assurance (QA) and Configuration Management (CM) "Spot Check" was performed. Following a review of the ES&S's QA and CM documents iBeta requested ten work products in the areas of Product Development, Software Change Management, Hardware Change, Manufacturing, and Fielded Product. Work products included documents, screen shots, reports, or other viewable file(s). Of the ten documents, initially, seven were found to conform to ES&S's QA and CM Plan documentation. The remaining three were accepted as consistent after the following clarification:

- iBeta requested a specific Engineering Change Order (ECO 841). The format of the ECO did not match section 9.7.1 of v. 3.0 of the CM Plan. ECOs can be generated from different entities. The example only identified the format of a single supplier. ES&S updated sections 9.7.1 and 9.7.2 to clarify other ECO formats. This is noted in Informational issue #179.
- iBeta requested a screen shot of the E-Synergy system process flow for ECO 841. It did not show evidence of SVP systems and Project Office approval for release to the VSTL (section 4.3, CM Plan v.3.0). ES&S clarified that hardware system changes and ECOs are approved. Release to the VSTL is a status tracked by the system and not a separate approval. This clarification was documented in sections 4.3.1 and 4.3.2.2 of the CM Plan, and the ECO Policies and Procedures v.2.0. This is noted in Informational issue #180.
- A test case was requested documenting ES&S' testing of a bug report. BUG16384. The reviewer found the test was appropriate for the issue but it did not have a cross reference identifying the bug number. ES&S provided System Change Notes v.13 that mapped BUG16384 to the test case. It was accepted as consistent.

### **5.2.1    *Unity 3.2.1.0 TDP Document Review Results***

The Technical Data Package was found to comply with the requirements of Vol. 2 Sect. 2 of the VSS 2002 and VVSG 2005. The documents accepted as compliant and the reviewed requirements are found in [Appendix C - PCA TDP Documentation Review](#).

The QA and CM observations and spot check found that overall the policy and processes were consistent. Noted version errors and minor CM Plan inconsistencies were noted as Informational discrepancies in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#)

## **5.3 FCA Functional System Level, Accessibility, Maintainability, Accuracy & Reliability Testing and Reuse of Testing**

There were three categories of functional testing for Unity 3.2.1.0.

- The first was the Functional System Level, Accessibility, Maintainability, Accuracy and Reliability testing of the M100 performed by SysTest in the Unity 4.0.0.0 test effort. Documentation of that testing is contained in the Summary Report of the testing performed by SysTest which is attached to the **ESSUnity3200** test report. (See [section 5.3.1](#).)
- The second category was performed to confirm the performance of the M100 integrated into the full voting system configuration of Unity 3.2.1.0. iBeta conducted a single regression end-to-end mock election which contained multiple test scenarios to demonstrate the integrated functionality and processes of the ES&S Unity 3.2.1.0. (See [section 5.3.2](#)). (It should be noted that additional functional system level test coverage was provided in the [section 5.4 Volume, Stress and Error Recovery](#) suite of tests.)
- The third category of functional testing involved testing of the ES&S functional enhancements and changes to the DS200 from the certified **ESSUnity3200**. These enhancements and changes were a result of internal ES&S testing, jurisdictions requests and field reports. A functional test case was created which contained multiple test scenarios. (See [section 5.3.3](#)). As a result of the changes submitted to address the field report of the DS200 freeze a DS200 Reliability Test was required. (See [section 5.3.4](#)).

Testing was conducted on the configuration identified in [Section 3.2 Voting System Test Environment](#). The applications were tested for the pre-vote and post vote election management system of the Unity 3.2.1.0 voting system and the voting/counting functionality of the AutoMARK VAT, M100, DS200, and M650 optical scanners.

### **5.3.1 EAC Evaluation for Reuse of the SysTest Labs Testing: M100 Functional, Accessibility, Maintainability, Accuracy & Reliability Test Results**

*Section 5.3.1 is provided by the EAC*

Due to the suspension of accreditation of a VSTL this project was moved from that VSTL to iBeta as requested by ES&S and approved by the EAC. This very unusual circumstance required that a transition plan be developed for the orderly transition of the project. A number of factors impacted the development of this transition plan.

The overriding consideration had to be that the quality of the evaluation meets the EAC's standards for excellence and that any decision to certify the system be clearly based on rigorous and thorough testing. If other legitimate concerns could also be met then every attempt was made to do so. Among those considerations was the timely evaluation of the system, avoiding duplicative testing that provided little real value and supporting the needs of election officials for improvements and upgrades.

In developing a transition plan a number of factors were taken into consideration:

1. The quality of testing already performed was evaluated. In some cases iBeta was directed to review or audit that testing. Another factor was the probability that testing to be performed by iBeta would identify any system issues that may have been missed in prior testing. In some cases iBeta was directed to modify the testing it would do to provide additional checks and redundancy in areas of particular concern.
2. Prior versions of this system are in wide use. In addition individual states and other organizations have conducted their own, independent evaluation of either this exact system or very similar prior versions. This provides a significant body of information from both experience in actual elections and testing performed for other purposes.

All of these sources of information were used in developing the transition plan. A risk assessment was made and a transition plan approved. This plan allowed for reuse of some testing, reuse of some testing after an audit and recommendation by iBeta, and requirements for further testing or correlated testing by iBeta.

The results of this evaluation were communicated to ES&S and iBeta in several E-Mails and letters between November 2008 and letters dated August 4, 2009, September 11, 2009, and March 24, 2010. In those communications the following was approved:

1. All hardware testing was approved for reuse.
2. The source code review was approved after a 3% audit and recommendation for reuse by iBeta.
3. The Volume, Stress, Error Recovery and Security test methods and testing had not yet been completed. Accordingly iBeta was to perform this testing on the Unity 3.2.1.0 system.

In order to determine the scope of the possible reuse of the functional, accessibility, maintainability, accuracy, and reliability testing conducted for the Unity 3.2.1.0. EAC technical reviewers conducted a full audit of all test plans, test methods, test cases, and test results related to the Unity 3.2.1.0 test campaign. This included a review of a document created by SysTest Labs that summarized all related testing conducted to date for the Unity 3.2.1.0 test campaign and provided the test results for that testing.

Determination of reuse of the Functional, Accessibility, Maintainability, Accuracy, and Reliability testing was provided by the EAC Technical Reviewer's following assessment of the test summary reports provided by SysTest on the M100 in the letter [03.24.10 Reuse of prior testing conducted by SysTest Laboratories](#).

1. All functional, accessibility, maintainability, accuracy, and reliability testing outlined in the approved SysTest Unity 4.0 test plan is approved for reuse in the Unity 3.2.1.0 test campaign.
2. As part of the remaining testing the EAC is tasking iBeta with testing and verifying that the Unity 3.2.1.0 system is in compliance with EAC RFI 2008-07 "0' count to start the election". This testing should be reflected in the test plan being developed by iBeta for the Unity 3.2.1.0 system.
3. iBeta is also tasked with testing the discrepancies listed by SysTest within the application for Unity 3.2.1.0.

### **5.3.2 Regression Functional & System Level Test Results**

iBeta performed a sampling single regression end-to-end mock election to demonstrate the integrated functionality and processes of the ES&S Unity 3.2.1.0. Additional functional system level test coverage was provided in the Volume suite of tests. Testing was conducted on the system configuration identified in Section 3. The application was tested for the pre-vote and post vote election management system of the Unity 3.2.1.0 voting system and the voting/counting functionality of the AutoMARK VAT, DS200 and M650 optical scanners.

The sampling was executed in six test scenarios. Tested requirements were traced to the applicable test cases in [Appendix A Certification Test Requirements](#). A description of the Regression Test Method and the acceptance or rejection of each test execution was provided in [Appendix D: Regression System Level Test Result](#). During testing functionality that did not meet the requirements of the VSS 2002 was rejected. Functional issues were recorded in the test case and reported to ES&S in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#). ES&S submitted fixes and the tests were rerun to verify acceptance.

[Appendix D Section 7.4.1.2 Regression System Level Test Results](#) provides a trace to the failures, errors, nonconformities and anomalies observed during testing and summarized in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#). The M100 Unity 4.0.0.0 issues that remained open at the time of transfer to iBeta were imported into [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#). They were traced to the original SysTest discrepancy number. Documentation of corrections and verification of corrections are contained in each issue summary.

### **5.3.3 DS200 Functional Enhancements and Changes Test Results**

iBeta verified the enhancements and changes to the DS200 submitted from the certified **ESSUnity3200** successfully met the VVSG 2005 requirements applicable to the modifications. The following are the DS200 Cosmetic and Functional Enhancements and Issues submitted for testing in Unity 3.2.1.0:

- BUG15827 Diverts Over Voted Write-ins
- BUG16775 L&A test decks displaying incorrect vote totals "scanning ballots with a contest in either Column C or D was reporting false results". (See Table 18 [Appendix H Amended Test Plan](#), for description.)
- BUG16782 Same as BUG16775
- BUG17666 Add protected count to status report (State of Maryland)
- BUG18361 Scanner performance

- BUG18687 Resolved issue of contest and candidates not appearing on the Zero Report
- BUG19664 Resolved error messages that can be logged into the internal log
- BUG19853 Resolved ballots being accepted after Audit Log is Full

ENHs are cosmetic and functional enhancements submitted by ES&S. These include:

- ENH14725 Display an "X" over the Image Icon if images are not being saved
- ENH14726 Extend the time "Thank you for voting" displays
- ENH14728 Modem transmission (modem use is out of scope of Unity 3.2.1.0)
- ENH14729 Permit multiple zero tapes to be printed before the first ballot is cast
- ENH14730 Change continuous alert beeping to just two beeps
- ENH14731 Provide an audible signal when ballot is accepted
- ENH14732 Repeat the machine ID and poll number at the end of the results tape
- ENH14745 Provide an override for Over Vote or blank ballot rejection
- ENH15009\* Implement Counterfeit Ballot Sensor (functionality withdrawn)
- ENH15287 Add Early Voting Ballot Styles per Precinct Report
- ENH15288 Increase the font size of the "Thank you for Voting" message
- ENH15418 Small white dots "speckling" in the timing tracking generating error
- ENH15890 Implement new scanner board firmware
- ENH15891\* Implement a new administration calibration function for ENH15009
- ENH15892 Update the scanner client to work with the new scanner board firmware
- ENH16085 Add new icons on the "Welcome" screen
- ENH16120 Change Over Vote warning screen text
- ENH16211 Print Machine ID & Poll Number in the Audit Log
- ENH16291 Additional language translations text for the Over Vote screen
- ENH16231 Write the administrative audit log entries as they occur
- ENH16336 Update language translations for the Over Vote screen
- ENH16382 Expand all election day capacity to 18 precincts
- ENH17266 Updated scanner board version
- ENH17268 Changed DS200 Firmware version from 1.3.x.x to 1.4.x.x (Florida version)
- ENH17538 Add Protected count DS200 Firmware and to reside on the compact flash card
- ENH18150 Test build to confirm protected counter is not deleted
- ENH18865 Add functionality to check the CRC on the USB Flash drive
- ENH19168 Add audit log entry for each time the DS200 casts a ballot
- ENH19169 Add audit log entry for each time the DS200 powers up
- ENH19170 Add audit log entry for each time the DS200 powers off
- ENH19323 Disable Counterfeit Detection
- ENH19663 Modem status added to Audit Log
- ENH19936 Resolved incorrect firmware version after firmware update on initial configuration

\* Note: The EAC has issued instructions to ES&S to disable DS200 code associated with the withdrawn counterfeit sensor. ENH19323 disables the functionality of ENH15009 and 15891.

This functional testing was executed in multiple test scenarios 1 – 7 and 9 – 11. Tested VVSG 2005 requirements and were traced to the applicable test cases, as noted in [Appendix A Certification Test Requirements](#). A description of the DS200 Functional Test Method and the acceptance or rejection of each test execution is provided in [Appendix D: DS200 Functional Test Result](#). During testing two issues (#132 and #143) were noted. These were rejected, recorded in the test case and reported to ES&S. ES&S provide a response to #132 which was retested and accepted. Failure of a fix submitted for #143 resulted in the withdrawal of enhancement ENH15009. [Appendix D: DS200 Functional Test Result](#) are cross referenced to these issues summarized in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#). The list below are enhancements and bugs that were not tested. **Scenario 8** had the following bug and enhancements:

#### **Scenario 8**

The DS200 system freeze and shut down functional enhancements were to be functionally tested in Scenario 8. This test scenario was not executed by November 29, 2010 because it was ES&S' intention to submit additional code enhancements. The freeze and shut down enhancements include:

- ENH18296 - reset the pointer used to free allocated memory to a "NULL" state after memory is freed, to prevent a "double free" memory condition

- ENH18555 - added event log entries for a condition where the DS200 is shut down while awaiting a voter response to a “hold ballot” event (blank ballot, overvote, etc.). This “hold ballot” event can occur when the ballot is delayed in the read path under any selected ballot handling configuration (‘query voter,’ automatic acceptance or automatic rejection)
- ENH18562 - added functionality to gracefully shut the system down in the event menus terminate unexpectedly
- ENH18681 - disabled screen hibernation between voters
- ENH18807 - added a screen message that displays upon recovering from a condition in which the DS200 is shut down while awaiting a voter response to a “hold ballot” event
- ENH18851 - The 7.5 version of the X-Windows system from xorg, fixed a problem that the DS200 had with the unexpected shutdowns. The new X-Windows system was incorporated into the OS. The new OS version moved from 1.0.1.0 to 1.0.2.0. Calls to X-Windows in the DS200 firmware include:
  - generating X events to simulate keyboard button presses
  - generating keyboard events sent to X server, convert X-server character values and printable character values
  - creating the calibration window and the Recalibrate and Exit buttons
  - functions for X server to load/unload the drive

#### **5.3.4 FCA DS200 Reliability Test Results**

In April of 2010 an issue involving the DS200 Intermittent Freeze/ Shut Down was identified during Logic and Accuracy testing in Cuyahoga County, Ohio for their May primary. (See the EAC [Voting System Technical Advisory Intermittent Freeze/Shutdowns with EAC Certified ES&S Unity 3.2.0.0 System](#)). As a result of the analysis and changes submitted (See section 2.1.5.2 DS200 Field Issue –Freeze and Shutdowns in [Appendix H Amended Test Plan](#)) Reliability testing of the DS200 was required.

The test was scheduled to run eight days (64 hours) on three units. Testing required that the DS200's operate for the full period of time without a loss of one or more functions or degradation of performance such that the device was unable to perform its intended function for longer than ten seconds. On the third day execution of the DS200 Reliability test was halted due to an issue encountered during test script iteration #67. The following observation report was provided to the EAC:

- 1) *“After the first ballot was cast a second ballot was inserted in the DS200.*
- 2) *The ballot was an open primary with a vote in two parties (Cross Vote). This ballot issue was identified to the tester with the option to “Accept” or “Reject” the ballot. The tester selected “Accept” and the tester heard the ballot drop. (At this point the system has performed as “intended”).*
- 3) *The tester then observed the screen flash two messages. The first contained the word “issue”. The second contained the word “return”. The motor did not engage or attempt to return the ballot.*
- 4) *The voting system continued operation by resetting to the “Welcome” page. It was in a state to accept a new ballot.*
- 5) *The tester observed that the ballot counter did not increment (1 vote was displayed).*
- 6) *The tester, recorder, ESS and EAC representatives observed there were two ballots (voter 1 & voter 2) in the ballot box and the counter indicated a single vote.*
- 7) *The polls were closed. The reports were printed.*
- 8) *It was confirmed on the reports that only a single ballot was recorded. The Cross Vote audit log entry was not recorded, but a returned ballot entry was recorded in the audit log.*
- 9) *The system was shut down via the touch screen selection.*
- 10) *The system was restarted, polls were re-opened, and additional ballots were scanned and reported, without error.*

*At no time was it observed that the system lost one or more functions. It remained available. There was no time to repair.*

- The voting function was not lost because it reset to the “Welcome” page.
- The function of closing the polls was not lost.
- The function of printing the report was not lost.
- The function of the audit log was not lost because the incorrect message was written to the log.
- There was no loss of touch screen function.
- There was no loss of the shut down function.
- There was no observation of ten second degradation in performance of any operation.

*Observation of the two flash messages leads rather to a hypothesis that the firmware performed an unintended operation and not a failure as related to an MTBF as identified in v.1: 4.3.3.”*

After reading the iBeta observations of Unity 3.2.1.0 Reliability testing and the Analysis of Anomaly Found during Reliability Test from ES&S, the EAC made the following determination:

*“After reviewing the anomaly analysis presented by ES&S, we feel that the preliminary analysis indicating that the recent testing anomaly is not related to the previous freeze/shutdown issue is plausible. We do feel, however, that a significant amount of research and analysis remains to be done in order for ES&S to determine the root cause of the most recent anomaly. Our analysis of the observations on the Reliability Test Iteration #67 leads us to conclude that the screen flashing the word “return” without the motors engaging to return the ballot constitutes a “loss of function” and thus a failure under Section 4.3.3. In addition, we also believe that the ballot counter not incrementing a vote cast on the machine, accepted and deposited into the ballot box also reflects a loss of function.”*

iBeta subsequently confirmed in a source code review that the motor does not start if the system does not sense the presence of a ballot. However until ES&S provides a root cause analysis that can substantiate if the system diverted from the intended path that increments the counter the EAC decision leaves the validation of correction of the freeze/shut down issue unanswered.

[Appendix D](#) contains the documentation of the DS200 Reliability Testing. Discrepancy #187 observed in the DS200 Reliability Testing is summarized in [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#).

## 5.4 FCA M100 Volume, Stress, and Error Recovery Testing

System limit conditions were previously tested in the certified **ESSUnity3200**. There were no changes that impacted those previously tested system limits. The Volume Stress and Error Recovery Tests conducted in Unity 3.2.1.0 was on the M100. iBeta performed seven test cases with maximum and overloaded volume scenarios to test the M100 limit conditions that ES&S identified. In discussions with the EAC it was agreed that the Volume test scenarios would incorporate validation that the system could perform to the identified system limit. Stress and error recovery conditions would validate that appropriate responses were encountered for overloaded conditions. Appropriate responses were: 1) to handle the overload; 2) generate an error; or 3) if the system halts processing without generating an error, the system recovers without any loss of data.

Additionally error recovery was addressed in the source code review of the requirement v.1: 4.2.3.e which specifies a single exit point and SysTest Labs' power recovery test results which validated recovery from power or system failure without loss of vote data and the minimum two hour back-up power.

Testing by iBeta was conducted on the system configuration identified in [Section 3.2 Voting System Test Environment](#). The application was tested for the system limits, overload conditions and error recovery of the Unity 3.2.1.0 voting system and the voting/counting functionality of the M100 optical scanner.

### 5.4.1 FCA M100 Volume Stress and Error Recovery Test Results

iBeta confirmed that the M100 could process the maximum system limits documented by ES&S and appropriate responses were encountered for overloaded and error conditions.

[Appendix D FCA Volume Testing](#) details specific information on the Volume, Stress, and Error Recovery Test execution. The two issues (#65 and 67) observed during testing by iBeta are cross referenced to the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#). Documentation of issue, corrections and verification of corrections are contained in each issue summary.

## **5.5 FCA Security Review and Testing**

iBeta's security specialist, a Certified Information System Security Professional, supervised execution of a security analysis based on a threat model for the applicable Unity 3.2.1.0 Security TDP documents to the requirements of the VSS 2002 Vol.1 Sect. 2.2.1 a to -g, 2.2.2.1 d & e, 2.2.3 a-c, 2.2.4.1 e, f, g, i & j, 2.2.4.2, 2.2.5.3 , 4.5, and section 6. The Security Review assessed the required testing in two ways.

- First the analysis identified VSS 2002 security requirements that were currently addressed in the standard testing, source code and document reviews.
- Second, the analysis identified any unique voting system specific tests, source code and/or document reviews that would be required to test Unity 3.2.1.0 to the VSS 2002. Each test, source code review or document review was traced to the applicable VSS 2002 requirement in the FCA Security Review and Testing table. The review detail recorded in the table was then used to create the Security Test Method and Test Case. Results of the standard source code, document review or test were recorded in the applicable FCA Functional and System Integration Test Case, PCA Source Code Review or the PCA Document Review. The unique tests and reviews were documented in the FCA Security Review and Test Case. This documentation included the steps, acceptance and rejection criteria, and results. Appendix D contains the FCA Security Review and Test Methodology

In order to comply with the security test requirements identified in Vol.2 Sect. 6.4 of the VSS 2002. iBeta approached security testing of the VSS 2002 by first creating test scenarios which discounted the exposure to risk and excluded physical security procedures. However, in establishing acceptance and rejection criteria, iBeta assessed the potential exposure to risk and included physical security procedures as an acceptable security control, per the requirements of Vol. 1 Sect. 6.3 of the VSS 2002. To assess if an access control was effective iBeta considered the degree to which one or more of the following security controls was present:

- 1) Physical security procedures, password protection;
- 2) Detection in an audit;
- 3) Technical expertise required;
- 4) Obfuscation of sensitive material; and
- 5) Encryption of sensitive material.

In determining potential exposure to risk the security specialist considered access from the user and if the exposure was from a trusted user or non-trusted user. Systems were accepted as meeting the security requirements of the VSS 2002 if the security controls present were deemed effective to address the identified risk.

Testing was conducted on the system configuration identified in [Section 3.2 Voting System Test Environment](#). Security testing for the unmodified elements of the certified **ESSUNITY3200** did not warrant additional testing in Unity 3.2.1.0. Security test was conducted for the M100 and the EMS stand-alone, peer-to-peer and Windows Server 2003 configurations.

### **5.5.1 FCA Security Review and Testing**

The ES&S recommended security procedures and protocols for the Unity 3.2.1.0 system verified and met the applicable VSS 2002/ VVSG 2005 security requirements and mandate procedures for effective system security. Review and testing confirmed:

- The TDP mandates security procedures consistent with usage of the system and providing system integrity, availability, confidentiality and accountability.
- Pre-election election and ballot preparation tasks are unshared for any given election in EDM and ESSIM. Multiple read-only accesses of the election database are only permitted for the tasks associated with the generation of election media in HPM.
- Post-election usage of multiple ERM workstations may share the same election but are logically protected from modification at the precinct level.
- Usage of numbered seals and procedurally recording the numbers is mandated.

- ES&S provided procedures and hardening scripts for each of its configurations: XP stand-alone, peer-to-peer, and Windows Server 2003. Four roles define access to the Unity 3.2.1.0 system corresponding to a System Administrator, an Election Administrator, an Election Preparer and an Election Consolidation/Reporting Role. Privileges of the latter role may be restricted within ERM. Access to the stand-alone, peer-to-peer and client-server voting applications is controlled by the hardened BIOS and the hardened Windows operating systems. The hardened systems prevent execution of non-voting software and allow only authenticated users to access voting software. User access to files and execution of programs both locally and remotely appears in the Windows event log. Failure of the windows log prevents execution of voting software. Administrative permissions for the log are restricted to the system administrator.
- **ESSUNITY3200** was found consistent with the Security Content Automation Protocol (SCAP) check list, a NIST program to audit security settings in workstations and servers (RFI 2008-03). The peer-to-peer and Windows Server 2003 configurations were validated using the Nessus tool against the appropriate FDCC criteria. The stand-alone configuration was manually verified with a comparison to the checklist because the tool only works in a network environment.
- Access to incomplete election returns is controlled and write-back access to the election returns is denied to the user providing the returns.
- The networked election preparation and election reporting systems reside only on a physically isolated LAN. Even so penetration testing reported no vulnerabilities for the networked systems.
- Random pre-vote and post vote modifications to election data were detected by the M100, DS200 and by ERM.
- The M100 rejects random modifications to a firmware update.
- The M100 incorporates physical locks and seals to protect the installed and validated firmware and the installed election definition. Physical locks provide protection from voter and unauthorized personnel access to administrative functions.
- A PIN (in addition to the lock) prevents unauthorized access to re-open the polls on the M100.
- Access to M100 functionality or data through the serial port was denied. The M100 refused to execute a virus emulation program introduced via the PC card.
- Physical locks and seals protect the scanned ballots and ballot boxes.
- Known intermittent freezing and shutdown issues of the previously certified DS200 during L&A election testing were investigated by source code review and DS200 logging was enhanced to better address these issues when they occur in the field. Firmware modifications supporting the additional logging were regression tested.
- Through source code review analyzed code changes made to log all error events including halt conditions and designed tests for each branch of modified code. Three independent branches were found and functionally tested and the behavior was found to be the same as the previous version.
- There are two security issues, discrepancies #189 and 190 remain open as of November 29, 2010.

[Appendix D FCA Security Review and Testing](#) details specific information on the Security Review and Test execution. The security issues observed during testing by iBeta are cross referenced to the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#). Documentation of issue, corrections and verification of corrections are contained in each issue summary.

## 5.6 FCA Hardware Environmental Testing

Unity 3.2.1.0 voting system is composed of the previously certified **ESSUNITY3200** hardware (M650, AutoMARK VAT, and DS200) plus the M100 Precinct Count Scanner. The M100 was previously tested by SysTest as part of Unity 4.0.0.0 voting system. When SysTest's accreditation was suspended, the project was transferred to iBeta. As the M100 had not changed since completing hardware testing by SysTest, ES&S applied for reuse of the prior testing done by SysTest. The reuse was granted by the 8-4-2009 Letter to ESS.

The **ESSUNITY3200** certified M650 and AutoMARK VAT hardware was not changed and required no testing in Unity 3.2.1.0. Engineering change orders were submitted for the DS200, steel and plastic ballot boxes from the **ESSUNITY3200** certified baseline. The scope of any additional environmental testing was determined based upon an assessment of each ECO. Testing was to the VVSG 2005.

### **5.6.1 Changes to the DS 200 from the ESSUNITY3200 configuration**

The DS200 submitted 38 ECOs included changes to the plastic and steel ballot boxes, the DS200 scanner and documentation relevant to the manufacturing administrative process.

The administrative ECOs incorporated details such as label changes, production status changes, out of scope equipment, documentation changes and drawings. Minor changes to hardware that did not change the form, fit or function were submitted. (Example: changing the screw head pattern from a Slot to a Phillips.) These ECO's were reviewed and determined to have no impact that would require hardware environmental testing. This included ECOs 000315, 000337, 000342, 000366, 000375, 000423, 000466, 000523, 000545, 000554, 000562, 000566, 000570, 000582, 000618, 000628, 000665, 000669, 000674, 836, 837, 838, 839, 845, 846, 851 and 855.

Assessment of the testing required for 11 ECOs which impacted the electrical components of the DS200 scanner and ballot boxes are listed below. Changes to the DS200 were tested to the VSS 2002 and VVSG 2005. All tests are identical except the Electrical Fast Trans IEC 61000-4-4 (2004-07) Ed. 2 as identified in RFI 2008-10, which requires a Repetition Rate for all transient pulses at 100 kHz. No changes were identified as impacting transportation or storage.

The table below identifies the Engineering Change Orders that were further assessed by Criterion Technologies Inc. and their findings.

**Table 12 ECOs Impacting Electrical Components or Transportation & Storage**

ECO #	Description of ECOs	Operating- EMC	Non-operating Trans- portation & Storage
000332	DS200 Plastic Ballot Box new lock.	Yes - 4.8.3 Electrostatic Disruption EN-61000-4-2	No testing required
000339	Add washer & rivet to hold foam on the DS200 Ballot Box carry case	No testing required	No testing required
000359	DS200 Plastic Ballot Box Adding metal bottom edge	Yes - 4.8.3 Electrostatic Disruption EN-61000-4-2	No testing required
000529	DS200 Carry Case Remove micro switch bracket, and switch cable from the case	No testing required	No testing required
000534	DS200 add clamps to chassis	No testing required	No testing required
000535	DS200 Tape and holes for attaching clamps, no change to wire routing	No testing required	No testing required
000576	DS200 End of life SMT Power Inductor	No testing required	No testing required
841	DS200 Add Rod Lens Array, Capacitor, protected power switch	Yes -All EMC Tests	No testing required
843	Steel Ballot Box - Added a new diverter cable	Yes - All except 4.8.8 Magnetic Fields Immunity EN-61000-4-8	No testing required
844	DS200 End of life products replaced: 2 capacitors, 2 resistors and 1 diode	Yes - 4.8.3 Electrostatic Disruption EN-61000-4-2	No testing required
847	DS200 alternate LCD Backlight Inverter	Yes - All except 4.8.8 Magnetic Fields Immunity EN-61000-4-8	No testing required

The hardware environmental testing identified above included all of the above listed ECOs and was conducted by Criterion on the DS200 and ballot box system configurations identified in Section 3.

Engineering changes that did not require environmental retest or any other functional testing were approved as de minimus by the EAC. See the ES&S Correspondence on the EAC website [EAC Letter on De Minimus Changes to ESSUNITY3200](#). A listing of all hardware and software changes is found in [Appendix K 3.2.1.0 List of Changes Submitted in Unity 3.2.1.0](#).

### **5.6.2    *Electrostatic Disruption VSS 4.8.3 Testing on the M100***

In the Unity 4.0.0.0 certification effort SysTest determined that the M100 had been previously tested for non-EAC certifications by non-core hardware labs accredited in the VSS required environmental hardware test methods. EAC NOC 08-001 *Validity of Prior Non-Core Hardware Environmental and EMC Testing* permits reuse of non-core environmental testing if the VSTL, or designated sub contractor, re-runs the ESD test. This testing had been performed by SysTest but in a report review required by the EAC two document discrepancies (see Appendix E issues #1 and 2) were found in the reports. In order to expedite the test process ES&S withdrew their request to reuse the ESD report and asked that the test be re-run under iBeta's supervision. Testing of the M100 was conducted on the system configuration identified in Section 3.

### **5.6.3    *Hardware Environmental Tests and Test Results***

iBeta test staff observed the execution of the hardware tests conducted by Criterion. The DS200 successfully completed all EMC operating tests and all pre and post testing operational status check. M100 successfully completed the ESD test and all pre and post testing operational status check.

[Appendix D - HW Environmental](#) details specific information on the Hardware Environmental Testing.

## **5.7    *FCA Telephony and Cryptographic Review and Testing***

As noted in [Section 1.2 Unity 3.2.1.0 Exclusions](#) the voting system does not support public network data transmission for remote transmission of votes or consolidated results. The M100 modems were removed from this certification application. As such it is exempt from the Telecommunications requirements of Vol. 1 Sect. 5 & 6. The Telephony and Cryptographic Review and Testing were conducted to confirm the absence of network functionality.

### **5.7.1    *FCA Telephony and Cryptographic Review and Tests***

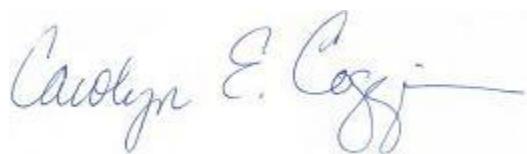
iBeta confirmed that the Unity 3.2.1.0 voting system election management hardware and installation procedures reflect the prohibition of connection of the certified system to a public network for the transmission of votes. The M100 equipment was inspected to confirm modem hardware was not present. (Similar testing of the M650 and DS200 is noted in the **ESSUNITY3200** Test Report.) Security Testing confirmed access to public telecommunications is not available through a modem attached through the serial port. Currently fielded DS200 and M100 may have internal modems installed. Installation of Unity 3.2.1.0 with those configurations is non-compliant with the EAC certification. [Appendix D Telephony and Cryptographic](#) details specific information on the Telephony and Cryptographic Review and Testing. No documentation errors, nonconformities or anomalies were observed.

## 6 Opinions & Findings

The results noted in this report identify the testing completed by iBeta Quality Assurance on the Unity 3.2.1.0 voting system as of November 29, 2010. At that time nine discrepancies remained open. These discrepancies are found in [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#) (#178, 181, 182, 187, 188, 189, 190, 191, and 192). Tests which were not completed include Scenario 8 of the DS200 Functional Test Case and the DS200 Reliability Test Case for the freeze and shut down field report.

In our opinion the acceptance requirements of the Federal Election Commission Voting System Standards April 2002 and applicable requirements of the Election Assistance Commission Voluntary Voting System Guidelines December 2005 identified in [Appendix A](#) as "Reject" have not been met. Requirements identified as "Accept" have been met.

iBeta Quality Assurance recommends that the Election Assistance Commission accept the opinions, test results, and findings of this report in considering certification of the Unity 3.2.1.0.



QA Director Voting  
December 13, 2010

## 7 APPENDICES: TEST OPERATION, FINDINGS & DATA ANALYSIS

The *Voting System Test Laboratory Program Manual v.1.0* Appendix B identifies content in specific appendices. In order to ensure that this content and content required by the VSS 2002 or VVSG 2005 for modifications to the **ESSUNITY3200** certified voting system Volume 2 Appendix B a trace is provided in [section 1.6.1](#) to clarify the location of this specified content

### 7.1 Appendix A- VSS 2002 and applicable VVSG 2005 Certification Test Requirements

Appendix A identifies the test results to the Certification Test Requirement of the VSS 2002 or VVSG 2005 for modifications to the **ESSUNITY3200** certified voting system. Requirements marked:

- Accept: met the requirement
- Reject: did not meet the requirement
- NA: the requirement is not applicable to the voting system type submitted for Certification Testing
- Pending: requirements that cannot be completed by the VSTL until after Certification
- Out of Scope: requirements which are performed by entities other than the VSTL

Requirements marked Reject, NA, Pending or Out of Scope shall include an explanatory note. (Example: If a voting system is only a Central Count Scanner, the requirement is marked "NA" and a comment indicates "Not a DRE.")

Optional requirements which apply to the voting system type but are not supported by the ES&S Unity 3.2.1.0 Voting System are not marked "NA". Instead they are marked "Accept", with an explanatory comment. The reason for this is to provide a positive identification that iBeta reviewed the voting system for all applicable requirements, including this optional functionality and confirmed non-support. (Example: If a voting system does not have a VVPAT. The requirements are marked "Accept" and a comment indicates "DRE does not have a VVPAT".)

The test case trace corresponds to the Test Methods identified in the Test Plan & [Appendix D](#):

#### Unity 3.2.1.0 = Testing in the Unity 3.2.1.0 Test Cases for the M100 and EMS LAN

- E-M100= Reuse Environmental & Reliability
- E-DS200= Environmental testing enhancements to DS200
- F-M100= Reuse SysTest Functional, Characteristics, Maintenance, Accessibility, Availability, Data Accuracy
- F-DS200= The DS200 Cosmetic and Functional Enhancements and Issues
- R3210= Regression System Level which includes both M100, EMS LAN and **ESSUNITY3200** unmodified hardware and software
- S3210= Security Test Case
- T3210= Telephony & Cryptographic Test Case
- V-M100 #= Volume M100 1, 2, 4, 5, 11, 12, or 13 Test Cases
- R-DS200= Reliability Test Case (incomplete as of 11/29/10)
- NA=The requirement is not applicable to the voting system type or is unmodified from **ESSUNITY3200**

#### **ESSUNITY3200 Unmodified= No changes, all testing is completed, the testing for results listed here is documented in the ESSUNITY3200 Test Report**

- E= Reuse Environmental & Reliability
- F= Reuse SysTest Functional, Characteristics, Maintenance, Accessibility, Availability, Data Accuracy
- R= Regression System Level
- S= Security Test Case
- T= Telephony & Cryptographic Test Case
- V1-10= Volume 1 through 10 Test Cases
- NA= The requirement is not applicable to the voting system type

Issues identified during testing are cross-referenced to the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#).

EAC Decisions on Requests for Interpretation which were applicable to the voting system submitted for certification testing are noted in the comments

Appendix A provides a map of the equipment type and features to the Volume 1 VSS 2002 and VVSG 2005 requirements. The *ES&S Unity 3.2.1.0 EAC Matrix* is provided as a separate document. This document identifies Volume 1 & 2 VSS 2002 and applicable VVSG 2005 requirements applicable to both the voting system and the VSTL test process. It is utilized by the VSTL and EAC in the certification test process review.

Manufacturer Voting System & Version	Scope	Prior EAC Certification#
ES&S Unity 3.2.1.0 Voting System	Initial M100 certification and EMS LAN (VSS 2002)	ESSUNITY3200

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
2.2	<b>Overall System Capabilities</b>					
2.2.1 VVSG 2005 2.1.1	<b>Security</b>  System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security all systems shall:					
a. VVSG 2005 a.	Provide security access controls that limits limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.	Accept	S3210, R3210	#58, 56, 57, 60, 70, 72, 75, 78, 79, 84, 86, 88, 93, 104, 105, 112, 126, 127, 136 - Closed	S	
b. VVSG 2005 b.	Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.	Reject	S3210, R3210, F-DS200	#187, 192 -Open  #52, 53, 55, 60, 68, 69, 71, 77, 78, 79, 80, 81, 82, 83, 88, 89, 123, 140, 143, 156, 172 - Closed	S, R	
c. VVSG 2005 c.	Use the system's control logic to prevent a system function from executing, if any preconditions to the function have not been met.	Accept	S3210, R3210	#53, 71, 78, 79, 89 - Closed	S, R	
d. VVSG 2005 d.	Provide safeguards to protect against tampering during system repair, or interventions in system operations, in response to system failure.	Accept	S3210	#78, 79 - Closed	S	
e. VVSG 2005 e.	Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation.	Reject	S3210, R3210, F-DS200	#178 - Open #53, 125 177 – Closed	S	
f. VVSG 2005 f.	If access to a system function is to be restricted or controlled the system shall incorporate the means of implementing this capability.	Reject	S3210, R3210, F-DS200	#178 –Open 177 – Closed	S	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
g. <b>VVSG 2005 g.</b>	Provide documentation of mandatory administrative procedures for effective system security.	Accept	S3210, R3210	#61, 78, 79, 148, 149, 150, 153, 154 - Closed	S	
2.2.2	<b>Accuracy</b> To ensure vote accuracy, all systems shall:					
2.2.2.1 <b>VVSG 2005 2.1.2</b>	Common Standards to Ensure Vote Accuracy To ensure vote accuracy, all systems shall:					
a. <b>VVSG 2005 a.</b>	Records the election contests, candidates, and issues exactly as defined by election officials.	Accept	F-M100, R3210		F, R	
b. <b>VVSG 2005 b.</b>	Records the appropriate options for casting and recording votes.	Accept	F-M100, R3210		F, R	
c. <b>VVSG 2005 c.</b>	Records each vote precisely as indicated by the voter and have the ability to produce an accurate report of all votes cast.	Reject	F-M100, R3210	#187 - Open RFI 2007-06	F, R	RFI 2007-06
d. <b>VVSG 2005 d.</b>	Control logic and data processing methods incorporation parity and check sums (or equivalent error detection and correction methods) to demonstrate the system has been designed for accuracy.	Accept	S3210	#160, 161, 162, 163 – Closed	S	
e. <b>VVSG 2005 e.</b>	The software monitors the overall quality of data read-write and transfer quality status, checks the number and types of errors that occur in any of the relevant operations on data and how they were corrected.	Accept	S3210		S	
2.2.2.2	DRE System Standards In additional DRE systems shall:					
	As an additional means of ensuring accuracy in DRE systems, voting devices record and retain redundant copies of the original ballot image. A ballot image electronic record of all votes cast by the voter, including undervotes.	Accept	NA	RFI 2007-06 No DRE	NA	RFI 2007-06 No DRE
2.2.3	<b>Error Recovery</b> To recover from a non-catastrophic failure of a device, or from any error or malfunction that is within the operator's ability to correct, the system shall provide the following capabilities:					
a. <b>VVSG 2005 a.</b>	Restoration of the device to the operating condition existing immediately prior to an error or failure, without loss or corruption of voting data previously stored in the device	Accept	F-DS200, F-M100, R3210, S3210, R-DS200, V-M100 1, 2, 4, 11, 12, 13		S, V1-10, R, F	
b. <b>VVSG 2005 b.</b>	Resumption of normal operation following the correction of a failure in a memory component, or in a data processing component, including the central processing unit	Reject	F-DS200, S3210, R3210, F-M100, R-DS200	#189 - Open	S, R, F	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
c. VVSG 2005 c.	Recovery from any other external condition that causes equipment to become inoperable, provided that catastrophic electrical or mechanical damage due to external phenomena has not occurred.	Accept	S3210, R3210, F-M100		S, R, F	
2.2.4 VVSG 2005 2.1.4	<b>Integrity</b> Integrity measures ensure the physical stability and function of the vote recording and counting processes. To ensure system integrity, all systems shall:					
2.2.4.1	Common Standards To ensure system integrity, all systems shall:					
a. VVSG 2005 a.	Protect against a single point of failure that would prevent further voting at the polling place.	Accept	F-M100		F	
b. VVSG 2005 b.	Protects against the interruption of electronic power.	Accept	F-M100, V-M100 5		F, V-5	
c. VVSG 2005 c.	Protects against electromagnetic radiation.	Accept	E-M100		E	
d. VVSG 2005 d.	Protects against the ambient temperature and humidity fluctuations.	Accept	E-M100		E	
e. VVSG 2005 e.	Protects against failure of any data input or storage device.	Accept	S3210, V-M100 4		S, V4	
f. VVSG 2005 f.	Protects against any attempt at improper data entry or retrieval	Accept	S3210, R3210	#53, 60, 71, 78, 79, 89 - Closed	S	
g. VVSG 2005 g.	Records and reports of any normal or abnormal events.	Reject	S3210, R3210, F-DS200, R-DS200	#188, 190 - Open #56, 57, 58 – Closed RFI 2009-04	S	
h. VVSG 2005 h.	Maintains a permanent record of original audit data that cannot be bypassed or turned off.	Accept	S3210	RFI 2009-04	S	
i. VVSG 2005 i.	Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator	Accept	R3210, F-DS200, R-DS200	RFI 2009-04 #184 - Closed	R	
j. VVSG 2005 j.	Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability	Accept	S3210, R3210 F-DS200		S	
2.2.4.2	DRE Systems Standards In addition to the common requirements, DRE systems shall:					
a.	Maintain a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path	Accept	NA	No DRE	NA	No DRE

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
b.	Provide a capability to retrieve ballot images in a form readable by humans	Accept	NA	No DRE	NA	No DRE
<b>2.2.5 VVSG 2005 2.1.5</b>	<b>System Audit</b> This section describes the context and purpose of voting system audits and sets forth specific functional requirements. Additional technical audit requirements are set for the in Section 4.					RFI 2008-12
<b>2.2.5.1 VVSG 2005 2.1.5</b>	System Audit Purpose and Context (see the VSS/VVSG for the full statement regarding purpose and context)					
<b>2.2.5.2 VVSG 2005 2.1.5.1.</b>	Operational Requirements					
	Audit records shall be prepared for all phases of election operations performed using devices controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records shall address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. The software shall activate the logging and reporting of audit data as described below.	Accept	S3210, R3210, F-M100, R-DS200		S, R, F	
<b>2.2.5.2.1 VVSG 2005 2.1.5.1.a</b>	Time, Sequence, and Preservation of Audit Records The timing and sequence of audit record entries is as important as the data contained in the record. All voting systems shall meet the requirements for time, sequence and preservation of audit records outlined below.					
<b>a. VVSG 2005 i.</b>	Except where noted, systems shall provide the capability to create and maintain a real-time audit record. This capability records and provides the operator or precinct official with continuous updates on machine status. This information allows effective operator identification of an error condition requiring intervention, and contributes to the reconstruction of election-related events necessary for recounts or litigation.	Accept	S3210, R3210, F-M100, F-DS200, R-DS200		S, R, F	
<b>b. VVSG 2005 ii.</b>	All systems shall include a real-time clock as part of the system's hardware. The system shall maintain an absolute record of the time and date or a record relative to some event whose time and data are known and recorded.	Accept	S3210, R3210, F-M100, F-DS200, R-DS200		S, R, F	
<b>c. VVSG 2005 iii.</b>	All audit record entries shall include the time-and-date stamp.	Accept	S3210, R3210, F-M100, F-DS200, R-DS200		S, R, F	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
d. VVSG 2005 iv.	The audit record shall be active whenever the system is in an operating mode. This record shall be available at all times, though it need not be continually visible.	Accept	S3210, R3210, F-M100, F-DS200, R-DS200	#185	S, R, F	
e. VVSG 2005 v.	The generation of audit record entries shall not be terminated or altered by program control, or by the intervention of any person. The physical security and integrity of the record shall be maintained at all times.	Accept	S3210, R3210, F-M100, F-DS200, R-DS200		S, R, F	
f. VVSG 2005 vi.	Once the system has been activated for any function, the system shall preserve the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed.	Accept	S3210, R3210, F-M100, F-DS200, R-DS200		S, R, F	
g. VVSG 2005 vii.  1) 2) 3)	The system shall be capable of printing a copy of the audit record. A separate printer is not required for the audit record, and the record may be produced on the standard system printer if all the following conditions are met: • The generation of audit trail records does not interfere with the production of output reports • The entries can be identified so as to facilitate their recognition, segregation, and retention • The audit record entries are kept physically secure	Accept	S3210, R3210, F-M100, F-DS200, R-DS200	#65 - Closed	S, R, F	
2.2.5.2.2 VVSG 2005 2.1.5.1.b	Error messages All voting systems shall meet the requirements for error messages below.					
a. VVSG 2005 i.	The voting system shall generate, store, and report to the user all error messages as they occur.	Accept	S3210, R3210, F-M100, F-DS200, V-M100-1, 2, 5, 11, 12, 13R-DS200		S, R, F	
b. VVSG 2005 ii.	All error messages requiring intervention by an operator or precinct official shall be displayed or printed clearly in easily understood language text, or by means of other suitable visual indicators.	Accept	S3210, R3210, F-M100, F-DS200, V-M100-1, 2, 5, 11, 12, 13 R-DS200		S, R, F	
c. VVSG 2005 iii.	When the voting system uses numerical error codes for trained technician maintenance or repair, the text corresponding to the code shall be self-contained or affixed inside the voting machine. This is intended to reduce inappropriate reactions to error conditions, and to allow for ready and effective problem correction.	Accept	S3210, R3210, F-M100, F-DS200, V-M100-1, 2, 5, 11, 12, 13 R-DS200		S, R, F	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
d. VVSG 2005 iv.	All error messages for which correction impacts vote recording or vote processing shall be written in a manner that is understandable to an election official who possesses training on system use and operation, but does not possess technical training on system servicing and repair.	Accept	S3210, R3210, F-M100, F-DS200, V-M100-1, 2, 5, 11, 12, 13 R-DS200		S, R, F	
e. VVSG 2005 v.	The message cue for all voting systems shall clearly state the action to be performed in the event that voter or operator response is required.	Accept	S3210, R3210, F-M100, F-DS200, R-DS200, V-M100-1, 2, 5, 11, 12, 13	#67, 77, 107 - Closed	S, R, F	
f. VVSG 2005 vi.	Voting system design shall ensure that erroneous responses will not lead to irreversible error.	Accept	S3210, R3210, F-M100, F-DS200, R-DS200, V-M100-1, 2, 5, 11, 12, 13		S, R, F	
g. VVSG 2005 vii.	Nested error conditions are corrected in a controlled sequence such that voting system status shall be restored to the initial state existing before the first error occurred.	Accept	S3210, R3210, F-M100, F-DS200, V-M100-1, 2, 5, 11, 12, 13 R-DS200		S, R, F	
2.2.5.2.3	Status Messages The Standards/Guidelines provide latitude in software design so that vendors can consider various user processing and reporting needs. The jurisdiction may require some status and information messages to be displayed and reported in real-time. Messages that do not require operator intervention may be stored in memory to be recovered after ballot processing has been completed.					
	The voting system shall display and report critical status messages using clear indicators or English language text. The voting system need not display non-critical status messages at the time of occurrence. Voting systems may display non-critical status messages (i.e., those that do not require operator intervention) by means of numerical codes for subsequent interpretation and reporting as unambiguous text.	Accept	S3210, R3210, F-M100, F-DS200, V-M100-1, 2, 5, 11, 12, 13 R-DS200		S, R, F	
	Voting systems shall provide a capability for the status messages to become part of the real-time audit record.	Accept	S3210, R3210, F-M100, F-DS200, V-M100-1, 2, 5, 11, 12, 13 R-DS200		S, R, F	
	The voting system shall provide a capability for a jurisdiction to designate critical status messages.	Accept	S3210, R3210, F-M100, F-DS200, V-M100-1, 2, 5, 11, 12, 13 R-DS200		S, R, F	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
2.2.5.3 <b>VVSG 2005 2.1.5.2</b>	COTS General Purpose Computer System Requirements See the standards for the context these requirements. Three operating system protections are required on all such systems on which election software is hosted.			RFI 2008-03 RFI 2008-12		RFI 2008-03 RFI 2008-12
	Authentication shall be configured on the local terminal (display screen and keyboard) and on all external connection devices ("network cards" and "ports"). This ensures that only authorized and identified users affect the system while election software is running.	Accept	R3210		S	
	Operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object. This ensures the accuracy and completeness of election data stored on the system. It also ensures the existence of an audit record of any person or process altering or deleting system data or election data.	Accept	S3210, R3210	#72, 73, 74, 84, 86, 90, 93, 99, 119 - Closed	S	
	The system shall be configured to execute only intended and necessary processes during the execution of election software. The system shall also be configured to halt election software processes upon the termination of any critical system process (such as system audit) during the execution of election software.	Accept	S3210, R3210	#71, 73, 81, 82, 89, 90, 91 - Closed	S	
<b>2.2.6</b>	<b>Election Management System</b>					
<b>VVSG 2005 2.1.6</b>	The Election Management System (EMS) is used to prepare ballots and programs for use in casting and counting votes, and to consolidate, report, and display election results. An EMS shall generate and maintain a database, or one or more interactive databases, that enables election officials or their designees to perform the following functions:	Accept	F-M100, R3210  F-M100 4, R3210		F, R	
a.	Define of the political subdivision boundaries and multiple election districts, as indicated in the system documentation.	Accept	F-M100, R3210 F-DS200		F, R	
b.	Identify of contests, candidates, and issues.	Accept	F-M100, R3210 F-DS200		F, R	
c.	Define of ballot formats and appropriate voting options.	Accept	F-M100, R3210 F-DS200		F, R	
d.	Generate ballots and election-specific programs for vote recording and vote counting equipment.	Accept	F-M100, R3210	#146, 20 - Closed	F, R	
e.	Install ballots and election-specific programs.	Accept	F-M100, R3210		F, R	
f.	Test that ballots and programs have been properly prepared and installed.	Accept	F-M100, R3210		F, R	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
g.	Accumulate vote totals at multiple reporting levels as indicated in the system documentation.	Accept	F-M100, R3210		F, R	
h.  VVSG 2005 2.1.6	Generate of post-voting reports per Section 2.5.  Generate of post-voting reports per Section 2.4.	Accept	F-M100, R3210 F-M100 R3210	#20 - Closed	F, R	
i.	Process and produce audit reports of the data indicated in Section 4.5.	Accept	F-M100, R3210		F, R	
<b>2.2.7</b>	<b>Accessibility</b>					
2.2.7.1	Common Standards See the standard for diagrams. The voting system meets the following conditions:					
a.	Where clear floor space only allows forward approach to an object, the maximum high forward reach allowed shall be 48inches. The minimum low forward reach is 15 inches.	Accept	F-M100	As applicable to precinct scanners	F	
b.	Where forward reach is over an obstruction with knee space below, the maximum level forward reach is 25 inches. When the obstruction is less than 20 inches deep, the maximum high forward reach is 48 inches. When the obstruction projects 20 to 25 inches, the maximum high forward reach is 44 inches.	Accept	F-M100	As applicable to precinct scanners	F	
c.	The position of any operable control is determined with respect to a vertical plane that is 48 inches in length, centered on the operable control, and at the maximum protrusion of the product within the 48-inch length.	Accept	F-M100	As applicable to precinct scanners	F	
d.	Where any operable control is10 inches or less behind the reference plane, have a height that is between 15 inches and 54 inches above the floor.	Accept	F-M100	As applicable to precinct scanners	F	
e.	Where any operable control is more than 10 inches and not more than 24 inches behind the reference plane, have a height between 15 inches and 46 inches above the floor.	Accept	F-M100	As applicable to precinct scanners	F	
f.	Have operable controls that are not more than 24 inches behind the reference plane.	Accept	F-M100	As applicable to precinct scanners	F	
2.2.7.2	DRE Standards for Accessibility DRE voting systems shall provide, as part of their configuration, the capability to provide access to voters with a broad range of disabilities. This capability shall:					
a.	Not require the voter to bring their own assistive technology to a polling place.	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
b.	Provide Audio information and stimulus that:					
b.1.	Communicates to the voter the complete content of the ballot.	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
b.2.	Provides instruction to the voter in operation of the voting device.	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
b.3.	Provides instruction so that the voter has the same vote capabilities and options as those provided by the system to individuals who are not using audio technology	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
b.4.	For a system that supports write-in voting, enables the voter to review the voter's write-in input, edit that input, and confirm that the edits meet the voter's intent.	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
b.5.	Enables the voter to request repetition of any system provided information.	Accept	NA	M100 is not a DRE #137 - Closed	F	VAT - Ballot marking only
b.6.	Supports the use of headphones provided by the system that may be discarded after each use	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
b.7.	Provides the audio signal through an industry standard connector for private listening using a 1/8 inch stereo headphone jack to allow individual voters to supply personal headsets	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
b.8.	Provides a volume control with an adjustable amplification up to a maximum of 105 dB that automatically resets to the default for each voter	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
c.	Provide, in conformance with FCC Part 68, a wireless coupling for assistive devices used by people who are hard of hearing when a system utilizes a telephone style handset to provide audio information	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
d.	Meet the requirements of ANSI C63.19-2001 Category 4 to avoid electromagnetic interference with assistive hearing devices	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
e.	For Electronic Image Displays, permit the voter to:					
e.1.	Adjust contrast settings	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
e.2.	Adjust color settings, when color is used	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
e.3.	Adjust the size of the text so that the height of capital letters varies over a range of 3 to 6.3 millimeters	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
f.	For a device with touch screen or contact-sensitive controls, provide an input method using mechanically operated controls or keys that shall:					
f.1.	Be tactilely discernible without activating the controls or keys.	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
f.2.	Be operable with one hand and not require tight grasping, pinching, or twisting of the wrist.	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
f.3.	Require a force less than 5 lbs (22.2 N) to operate.	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
f.4.	Provide no key repeat function.	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
g.	For a system that requires a response by a voter in a specific period of time, alert the voter before this time period has expired and allow the voter additional time to indicate that more time is needed	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
h.	For a system that provides sound cues as a method to alert the voter about a certain condition, such as the occurrence of an error, or a confirmation, the tone shall be accompanied by a visual cue for users who cannot hear the audio prompt	Accept	NA	M100 is not a DRE	F	VAT - Ballot marking only
i.	Provide a secondary means of voter identification or authentication when the primary means of doing so uses biometric measures that require a voter to possess particular biological characteristics	Accept	NA	M100 is not a DRE	F	VAT has no biometric measures
<b>2.2.8</b>	<b>Vote Tabulating Program</b>					
2.2.8.1	Functions The vote tabulating program software resident in each voting machine, vote count server, or other devices shall include all software modules required to:					
a.	Monitor of system status and generating machine-level audit reports	Accept	F-M100, R3210	#65, - Closed	F, R	
b.	Accommodate device control functions performed by polling place officials and maintenance personnel	Accept	F-M100, R3210		F, R	
c.	Register and accumulating votes	Accept	F-M100, R3210		F, R	
d.	Accommodate variations in ballot counting logic	Accept	F-M100, R3210		F, R	
2.2.8.2	Voting Variation The Technical Data Package accompanying the system shall specifically identify which of the following items can and cannot be supported by the voting system, as well as how the voting system can implement the items support.					
a.	Documented support or non-support of closed primaries.	Accept	F-M100, V-M100 1		F	
b.	Documented support or non-support of open primaries.	Accept	F-M100, R3210 F-DS200		F	
c.	Documented support or non-support of partisan offices.	Accept	F-M100, R3210 F-DS200		F	
d.	Documented support or non-support of non-partisan offices.	Accept	F-M100, R3210		F	
e.	Documented support or non-support of write-in voting.	Accept	F-M100, R3210 F-DS200		F	
f.	Documented support or non-support of Primary presidential delegation nomination.	Accept	F-M100		F	
g.	Documented support or non-support of ballot rotation.	Accept	F-M100		F	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
h.	Documented support or non-support of straight party voting.	Accept	F-M100		F	
i.	Documented support or non-support of cross-party endorsement	Accept	F-M100		F	
j.	Documented support or non-support of split precincts.	Accept	F-M100, R3210		F	
k.  VVSG 2005 2.1.7.2	Documented support or non-support of vote for N of M.	Accept	F-M100, R3210 F-DS200		F	
l.	Documented support or non-support of recall issues, with options.	Accept	F-M100		F	
m.	Documented support or non-support of cumulative voting.	Accept	Doc Review	Not supported	F	
n.	Documented support or non-support of ranked over voting.	Accept	Doc Review	Not supported	F	
o.	Documented support or non-support of provisional or challenged ballots.	Accept	Doc Review	Election procedure	F	
2.2.9	<b>Ballot Counter</b> For all voting systems, each device that tabulates ballots shall provide a counter that:..					
a.	Can be set to zero before any ballots are submitted for tally	Accept	F-M100, R3210		F, R	
b.	Records the number of ballots cast during a particular test cycle or election	Reject	F-M100, R3210	#187	F, R	
c.	Increases the count only by the input of a ballot	Accept	F-M100, R3210		F, R	
d.	Prevents or disables the resetting of the counter by any person other than authorized persons at authorized points	Accept	F-M100		F	
e.	Is visible to designated election officials	Accept	F-M100, R3210		F, R	
2.2.10  VVSG 2005 2.1.9	<b>Telecommunications</b> For all voting systems that use telecommunications for the transmission of data during pre-voting, voting or post-voting activities, capabilities shall be provided that ensure data are transmitted with no alteration or unauthorized disclosure during transmission. Such transmissions shall not violate the privacy, secrecy, and integrity demands of the Standards. Section 5 of the Standards describes telecommunications standards that apply to, at a minimum, the following types of data transmissions:					
	Voter Authentication: Coded information that confirms the identity of a voter for security purposes for a system that transmit votes individually over a public network	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
	Ballot Definition: Information that describes to voting equipment the content and appearance of the ballots to be used in an election	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
	Vote Transmission to Central Site: For voting systems that transmit votes individually over a public network, the transmission of a single vote to the county (or contractor) for consolidation with other county vote data	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
	Vote Count: Information representing the tabulation of votes at any one of several levels: polling place, precinct, or central count	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
	List of Voters: A listing of the individual voters who have cast ballots in a specific election	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
2.2.11	<b>Data Retention</b> See standard/guideline for context.					
	All voting systems shall provide for maintaining the integrity of voting and audit data during an election and for a period of at least 22 months thereafter.	Accept	Doc Review		TDP	Attestation from ESS
2.3	<b>Pre-voting Functions</b>					#50 Closed
2.3.1	<b>Ballot Preparation</b>					
2.3.1.1 <b>VVSG 2005</b> 2.2.1.1	General Capabilities					
	All systems shall provide the general capability for ballot preparation, ballot formatting and ballot production. All systems shall be capable of:	Accept	F-M100, R3210 F-DS200		F, R	
2.3.1.1.1	Common Standards All systems shall be capable of:					
a.	Enable the automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed on the ballot for each political subdivision and election district.	Accept	F-M100, R3210		F, R	
b. 1) 2) 3)	Collecting and maintaining the following data: Offices with labels/instructions Candidate names with labels Issues or measures with their text	Accept	F-M100, R3210		F, R	
c.	Supporting the maximum number of potentially active voting positions as indicated in the system documentation.	Accept	NA	Unmodified from <b>ESSUNITY3200</b>	F, V8	
d.	For a primary election, generating ballots that segregate the choices in partisan races by party affiliation	Accept	F-M100, R3210		F, R	
e.	Generating ballots that contain identifying codes or marks uniquely associated with each format.	Accept	F-M100, R3210		F, R	
f.	Ensuring voter response fields, selection buttons, or switches properly align with the specific candidate names and/or issues printed on the ballot display, ballot card or sheet, or separate ballot pages.	Accept	F-M100, R3210		F, R	
2.3.1.1.2	Paper-Based System Standards Paper-based voting systems shall also meet the following requirements applicable to the technology used.					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
a. VVSG 2005 g.	Enable voters to make selections by punching a hole or by making a mark in areas designated for this purpose upon each ballot card or sheet.	Accept	F-M100, R3210 F-DS200		F, R	
b.	For punchcard systems ensure that the vote response fields can be properly aligned with punching devices used to record votes.	Accept	NA	M100 is not a punchcard system	NA	Not a punchcard system
c. VVSG 2005 h.	For marksense systems, the timing marks align properly with the vote response fields.	Accept	F-M100, R3210 F-DS200		F, R	
2.3.1.2	Ballot Formatting All voting systems shall provide a capability for:					
a.	Creation of newly defined elections	Accept	F-M100, R3210		F, R	
b.	Rapid and error-free definition of elections and their associated ballot layouts	Accept	F-M100, R3210		F, R	
c.	Uniform allocation of space and fonts used for each office, candidate, and contest such that the voter perceives no active voting position to be preferred to any other.	Accept	F-M100, R3210		F, R	
d.	Simultaneous display of the maximum number of choices for a single contest as indicated by the vendor in the system documentation	Accept	F-M100		F	
e.	Retention of previously defined formats for an election	Accept	F-M100, R3210		F, R	
f.	Prevention of unauthorized modification of any ballot formats	Accept	F-M100, R3210		F, R	
g.	Modification by authorized persons of a previously defined ballot format for use in a subsequent election	Accept	F-M100, R3210, V-M100 4		F, V3 & 4	
2.3.1.3	Ballot Production Ballot production is the process of converting ballot formats to a media ready for use in the physical ballot production or electronic presentation.					
VVSG 2005 2.2.1.3	Ballot Production Ballot production is the process of converting ballot formats to a media ready for use in the physical ballot production or electronic presentation.  The voting system shall provide a means of printing or other wise generating a ballot display that can be installed in all system voting devices for which it is intended: All systems shall provide the capabilities below					
2.3.1.3.1	Common Standards The voting system shall provide a means of printing or other wise generating a ballot display that can be installed in all system voting devices for which it is intended: All systems shall provide a capability to ensure.					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
a.	The electronic display or printed document on which the user views the ballot is capable of rendering an image of the ballot in any of the languages required by The Voting Rights Act of 1965, as amended	Accept	F-M100, R3210	RFI 2008-04	F	RFI 2008-04
b.	The electronic display or printed document where the user views the ballot does not show any advertising or commercial logos of any kind, whether public service, commercial, or political, unless specifically provided for in State law. Electronic displays do not provide connection through hyperlink.	Accept	F-M100		F	
c.	The ballot conforms to vendor specifications for type of paper stock, weight, size, shape, size and location of punch or mark field used to record votes, folding, bleed through, and ink for printing if paper ballot documents or paper displays are part of the system	Accept	F-M100, R3210		F, R	
2.3.1.3.2	Paper-based System Standards					
VVSG 2005 2.2.1.3	Vendor documentation for marksense systems shall include specifications for ballot materials to ensure that vote selections are read from only a single ballot at a time, without detection of marks from multiple ballots concurrently (e.g., reading of bleed-through from other ballots)	Accept	F-M100, F-DS200		F	
2.3.2	<b>Election Programming</b> Process by which election officials or their designees use election databases and vendor system software to logically define the voter choices associated with the contents of the ballots. All systems shall provide for:					
a.	Logical definition of the ballot, including the definition of the number of allowable choices for each office and contest	Accept	F-M100, R3210		F, R	
b.	Logical definition of political and administrative subdivisions, where the list of candidates or contests varies between polling places	Accept	F-M100, R3210		F, R	
c.	Exclusion of any contest on the ballot in which the voter is prohibited from casting a ballot because of place of residence, or other such administrative or geographical criteria	Accept	F-M100, R3210		F, R	
d.	Ability to select from a range of voting options to conform to the laws of the jurisdiction in which the system will be used	Accept	F-M100, R3210		F, R	
e.	Generation of all required master and distributed copies of the voting program, in conformance with the definition of the ballots for each voting device and polling place, and for each tabulating device	Accept	F-M100, R3210		F, R	
2.3.3	<b>Ballot and Program Installation and Control</b> All systems shall include the following at the time of ballot and program installation:	Accept				

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
	All systems provide a means of installing ballots and programs on each piece of polling place or central count equipment according to the ballot requirements of the election and the jurisdiction.	Accept	F-M100, R3210	#107 - Closed	F, R	
a.	A detailed work plan or other documentation providing a schedule and steps for the software and ballot installation, including a table outlining the key dates, events and deliverables.	Accept	F-M100, R3210		F	
b.	A capability for automatically verifying that the software has been properly selected and installed in the equipment or in programmable memory devices and for indicating errors.	Accept	F-M100, S3210, R3210		F,S	
c.	A capability for automatically validating that software correctly matches the ballot formats that it is intended to process, for detecting errors, and for immediately notifying an election official of detected errors.	Accept	F-M100, S3210, R3210		F, S	
2.3.4	<b>Readiness Testing</b> Election personnel conduct voting equipment and voting system readiness tests prior to the start of an election to ensure that the voting system functions properly, to confirm that voting equipment has been properly integrated, and to obtain equipment status reports. All voting systems shall provide the capabilities to					
2.3.4.1	Common Standards All voting systems shall provide the capabilities to:					
a.	Verify the voting machines or vote recording and data processing equipment, precinct count equipment, and central count equipment are properly prepared for an election, and collect data that verifies equipment readiness	Accept	F-M100, S3210, R3210, V-M100-1, 2, 11, 12		F, S	
b. <b>VVSG 2005 2.2.4.b</b>	Obtains status and data reports from each set of equipment	Accept	F-M100, R3210 F-DS200, V-M100-1, 2, 11, 12		F, R	
c.	Verify the correct installation and interface of all system equipment	Accept	F-M100, R3210, V-M100-1, 2, 11, 12		F, R	
d.	Verify that hardware and software function correctly	Accept	F-M100, R3210, V-M100-1, 2, 11, 12		F, R	
e.	Generate consolidated data reports at the polling place and higher jurisdictional levels	Accept	F-M100, R3210, V-M100-1, 2, 11, 12		F, R	
f.	Segregate test data from actual voting data, either procedurally or by hardware/software features	Accept	F-M100, R3210, V-M100-1, 2, 11, 12		F, R	
	Resident test software, external devices, and special purpose test software connected to or installed in voting devices to simulate operator and voter functions used for these tests meeting the following standards:					
a.	These elements are capable of being tested separately, and are proven to be reliable verification tools prior to their use	Accept	F-M100		F	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
b.	These elements are incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase.	Accept	F-M100		F	
2.3.4.2	Paper-Based Systems Paper-based systems shall:					
a.	Supports conversion testing that uses all potential ballot positions as active positions	Accept	F-M100		F	
b.	Supports conversion testing of ballots with active position density for systems without pre-designated ballot positions	Accept	F-M100		F	
2.3.5	<b>Verification at the Polling Place</b> All systems shall provide a formal record of the following, in any media, upon verification of the authenticity of the command source:					RFI 2008-07
a.	The election's identification data;	Accept	F-M100, R3210		F, R	
b.	The identification of all equipment units;	Accept	F-M100, R3210		F, R	
c.	The identification of the polling place;	Accept	F-M100, R3210		F, R	
d.	The identification of all ballot formats;	Accept	F-M100, R3210		F, R	
e.	The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros);	Accept	F-M100, R3210, S3210		F, R, S	
f.	A list of all ballot fields that can be used to invoke special voting options	Accept	F-M100		F	
g.	Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements	Accept	F-M100, R3210		F, R	
	To prepare voting devices to accept voted ballots, all voting systems shall provide the capability to test each device prior to opening to verify that each is operating correctly. At a minimum the tests shall include.	Accept	F-M100, R3210		F, R	
a.	Confirmation that there are no hardware or software failures.	Accept	F-M100, R3210		F, R	
b.	Confirmation that the device is ready to be activated for accepting votes.	Accept	F-M100, R3210		F, R	
	If a precinct count system includes equipment for the consolidation of polling place data at one or more central counting locations, it shall have means to verify the correct extraction of voting data from transportable memory devices, or to verify the transmission of secure data over secure communication links.	Accept	F-M100, R3210	Disabled M100 telecommunication in Unity 3.2.1.0	F, R	Telecommunication is disabled in <b>ESSUNITY3200</b>

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
2.3.6	<b>Verification at Central Location</b> Election officials perform verification at the central location to ensure that vote counting and vote consolidation equipment and software function properly before and after an election. Upon verification of the authenticity of the command source, any system used in a central count environment shall provide a printed record of the following:			RFI 2008-07		RFI 2008-07
a.	The election's identification data	Accept	F-M100, R3210	Unmodified from <b>ESSUNITY3200</b>	F, R	
b.	The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros);	Accept	F-M100, R3210	Unmodified from <b>ESSUNITY3200</b>	F, R S	S - per v.2: 3.3.1
c.	Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements.	Accept	F-M100, R3210	Unmodified from <b>ESSUNITY3200</b>	F, R	
2.4	<b>Voting Functions</b> <b>All voting systems shall support</b> <ul style="list-style-type: none"> <li>Opening the polls</li> <li>Casting the ballot</li> <li>In addition, all DRE systems shall support: Activating the ballot</li> <li>Augmenting the election counter</li> <li>Augmenting the life-cycle counter</li> </ul>					
	Opening the polls	Accept	F-M100, R3210		F, R	
	Casting the ballot	Accept	F-M100, R3210		F, R	
	In addition, all DRE systems shall support: Activating the ballot	Accept	NA	M100 is not a DRE	F, R	
	Augmenting the election counter	Accept	NA	M100 is not a DRE	F, R	VAT
	Augmenting the life-cycle counter	Accept	NA	M100 is not a DRE	NA	No DRE
2.4.1. <b>VVSG2005 2.3.1</b>	<b>Opening the Polls</b> The capabilities required for opening the polls are specific to individual voting system technologies. At a minimum, the systems shall provide the functional capabilities indicated below.					RFI 2008-07
2.4.1.1	Opening the polling Place (Precinct Count Systems) To allow voting devices to be activated for voting, the system shall provide:					
. <b>VVSG 2005 2.3.1.1</b>	Precinct Count Systems To allow voting devices to be activated for voting, all precinct count systems shall provide:					
a	An internal test or diagnostic capability to verify that all of the polling place tests specified in 2.3.5 have been successfully completed	Accept	F-M100, R3210,S3210, F- DS200	S - per v.2: 3.3.1	F, R,S	S - per v.2: 3.3.1
<b>VVSG 2005 a.</b>	An internal test or diagnostic capability to verify that all of the polling place tests specified in 2.2.5 have been successfully completed	Accept	F-DS200, R3210	S - per v.2: 3.3.1	F, R,S	S - per v.2: 3.3.1
<b>VVSG 2005 b.</b>	Automatic disabling any device that has not been tested until it has been tested.	Accept	F-M100, R3210,S3210, F- DS200	S - per v.2: 3.3.1	F, R,S	S - per v.2: 3.3.1

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
2.4.1.2	Paper-Based System Standards The standards for opening the polling place for paper-based systems consists of common standards and additional standards that apply to precinct count paper-based systems.					
2.4.1.2.1	All Paper-Based systems To facilitate opening the polls, all paper-based systems shall include:					
<b>VVSG 2005 2.3.1.2</b>	Precinct Count Systems To facilitate opening the polls, all paper-based systems shall include:					
a. <b>VVSG 2005 a.</b>	A means of verifying ballot punching or marking devices are prepared and ready to used;	Accept	F-M100, R3210 F-DS200	No ballot punching	F, R	No ballot punching
b. <b>VVSG 2005 b.</b>	A voting booth or similar facility, in which the voter may punch or mark the ballot in privacy	Accept	F-M100	No ballot punching	F	No ballot punching
c. <b>VVSG 2005 c.</b>	Secure receptacles for holding voted ballots. Ballot boxes.	Accept	F-M100, R3210, S3210, F-DS200	M100	F, R, S	DS200
2.4.1.2.2	Precinct Count Paper-Based Systems In addition to the above requirements, all paper-based precinct count equipment shall include a means of:					
a. <b>VVSG 2005 d.</b>	Activating the ballot counting device.	Accept	F-M100, R3210 F-DS200		F, R	
b. <b>VVSG 2005 e.</b>	Verifying that the device has been correctly activated and is functioning properly	Accept	F-M100, R3210 F-DS200		F, R	
c. <b>VVSG 2005 f.</b>	Identifying device failure and corrective action needed.	Accept	F-M100, R3210 F-DS200		F, R	
2.4.1.3	DRE System Standards To facilitate opening the polls, all DRE systems shall include:					
a.	A security seal, a password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the poll-opening function	Accept	NA	M100 is not a DRE	F, R, S	VAT doesn't open polls; it just switches to election marking mode
b.	A means of enforcing the execution of steps in the proper sequence if more than one step is required	Accept	NA	M100 is not a DRE	F	
c.	A means of verifying the system has been activated correctly	Accept	NA	M100 is not a DRE	F, R	
d.	A means of identifying system failure and any corrective action needed	Accept	NA	M100 is not a DRE	F	
<b>2.4.2</b>	<b>Activating the Ballot (DRE Systems)</b> To activate the ballot, all DRE systems shall:					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
a.	Enable election officials to control the content of the ballot presented to the voter, whether presented in printed form or electronic display, such that each voter is permitted to record votes only in contests in which that voter is authorized to vote	Accept	NA	M100 is not a DRE	F, R	VAT ballot marking functionality
b.	Allow each eligible voter to cast a ballot	Accept	NA	M100 is not a DRE	F, R	
c.	Prevent a voter from voting on a ballot to which he or she is not entitled	Accept	NA	M100 is not a DRE #138 - Closed	F, R	
d.	Prevent a voter from casting more than one ballot in the same election	Accept	NA	M100 is not a DRE	F, R	Blank paper ballot required
e.	Activate the casting of a ballot in a general election	Accept	NA	M100 is not a DRE	F	
f.	Enable the selection of the ballot that is appropriate to the party affiliation declared by the voter in a primary election	Accept	NA	M100 is not a DRE	F, R	Appropriate blank paper ballot required
g.	Activate all parts of the ballot upon which the voter is entitled to vote	Accept	NA	M100 is not a DRE	F,R	Some controls in addition to the paper ballot
h.	Disable of all parts of the ballot upon which the voter is not entitled to vote	Accept	NA	M100 is not a DRE	F,R	Some controls in addition to the paper ballot
<b>2.4.3</b>	<b>Casting a Ballot</b>					
2.4.3.1	Common Standards To facilitate casting a ballot, all systems shall:					
<b>VVSG 2005 2.3.3.1</b>	Common Requirements To facilitate casting a ballot, all systems shall:					
a.	Provide text that is at least 3 millimeters high and provide the capability to adjust or magnify the text to an apparent size of 6.3 millimeters	Accept	F-M100		F	
b.	Protect the secrecy of the vote such that the system cannot reveal any information about how a particular voter voted, except as otherwise required by individual State law	Accept	F-M100, R3210 F-DS200		F, R	
c. <b>VVSG 2005 c.</b>	Record the selection and non-selection (undervote) of individual vote choices for each contest and ballot measure	Accept	F-M100, R3210 F-DS200		F, R	
d. <b>VVSG 2005 d.</b>	Record the voter's selection of candidates whose names do not appear on the ballot, if permitted under State law, and record as many write-in votes as the number of candidates the voter is allowed to select	Accept	F-M100, R3210 F-DS200		F, R	
e.	In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power	Accept	F-M100, V-M100 5		F, V5	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
f.	Provide the capability for voters to continue cast ballots in the event of a failure of a telecommunications connection within the polling place or between the polling place and any other location	Accept	S3210, T3210	No telecommunications in vote casting on the in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
2.4.3.2	<u>paper-based System Standards</u>					
2.4.3.2.1	All Paper-Based Systems All paper-based systems shall:					
<b>VVSG 2005 2.3.3.2</b>	Paper-based System Requirement All paper-based systems shall:					
a.	Allow the voter to easily identify the voting field that is associated with each candidate or ballot measure response	Accept	F-M100, R3210 F-DS200		F, R	
b.	Allow the voter to punch or mark the ballot to register a vote	Accept	F-M100, R3210		F, R	
<b>VVSG 2005 b.</b>	Allow the voter to mark the ballot to register a vote	Accept	F-DS200		F, R	
c.	Allow either the voter or the appropriate election official is able to place the voted ballot into the ballot counting device (precinct count systems) or a secure receptacle (central count systems)	Accept	F-M100, R3210 F-DS200		F, R	
d.	Protect the secrecy of the vote throughout the process	Accept	F-M100, R3210 F-DS200		F, R	
2.4.3.2.2	Precinct Count Paper-Based Systems In addition to the above requirements, all paper-based precinct count equipment shall include a means of:					
a.	Provide feedback to the voter identifies specific contests or ballot issues for which an overvote or undervote is detected	Accept	F-M100, R3210 F-DS200		F, R	
b.	Allow the voter, at the voter's choice, to vote a new ballot or submit the ballot 'as is' without correction	Accept	F-M100, R3210, F-DS200		F, R	
c.	Allow an authorized election official to turn off the capabilities defined in the two prior provisions.	Accept	F-M100		F	
<b>2.3.3.2 VVSG 2005 e.</b>	Provide feedback to the voter that identifies specific contests for which he or she has made no selection or fewer than the allowable number of selections (e.g., undervotes)	Accept	F-DS200	2005 Requirement – DS200 testing		
<b>VVSG 2005 f.</b>	Notify the voter if he or she has made more than the allowable number of selections for any contest (e.g., overvotes)	Accept	F-DS200	2005 Requirement – DS200 testing		
<b>VVSG 2005 g.</b>	Notify the voter before the ballot is cast and counted of the effect of making more than the allowable number of selections for a contest	Accept	F-DS200	2005 Requirement – DS200 testing		
<b>VVSG 2005 h.</b>	Provide the voter opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted	Accept	F-DS200	2005 Requirement – DS200 testing		
2.4.3.3	DRE Systems Standards					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
a.	Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources)	Accept	NA	M100 is not a DRE	F,S	VAT ballot marking
b.	Enable the voter to easily identify the selection button or switch, or the active area of the ballot display that is associated with each candidate or ballot measure response	Accept	NA	M100 is not a DRE	F, R	VAT ballot marking
c.	Allow the voter to select his or her preferences on the ballot in any legal number and combination	Accept	NA	M100 is not a DRE	F, R	VAT ballot marking
d.	Indicate that a selection has been made or canceled	Accept	NA	M100 is not a DRE	F, R	VAT ballot marking
e.	Indicate to the voter when no selection, or an insufficient number of selections, has been made in a contest (e.g. undervotes)	Accept	NA	M100 is not a DRE	F, R	VAT ballot marking
f.	Prevent the voter from overvoting	Accept	NA	M100 is not a DRE	F, R	VAT ballot marking
g.	Notify the voter when the selection of candidates and measures is completed	Accept	NA	M100 is not a DRE	F, R	VAT ballot marking
h.	Allowing the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast	Accept	NA	M100 is not a DRE	F, R	VAT ballot marking
i.	For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot	Accept	NA	M100 is not a DRE	F, R	VAT ballot marking; printing is irrevocable but not casting of the ballot
j.	Notify the voter after the vote has been stored successfully that the ballot has been cast	Accept	NA	M100 is not a DRE		No DRE
K	Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear instruction as to the steps the voter should take to cast his or her ballot should this event occur	Accept	NA	M100 is not a DRE		No DRE
l.	Provides sufficient computational performance to provide responses back to each voter entry in no more than three seconds	Accept	NA	M100 is not a DRE	F	VAT ballot marking; printing exceeds 3 seconds
m.	The votes stored accurately represent the actual votes cast	Accept	NA	M100 is not a DRE	F, R	Storage is ballot printing
n.	Preventing modification of the voter's vote after the ballot is cast	Accept	NA	M100 is not a DRE	S	Paper ballot handling documentation
o.	Provides a capability to retrieve ballot images in a form readable by humans (in accordance with the requirements of Section 2.2.2.2 and 2.2.4.2)	Accept	NA	M100 is not a DRE		No DRE
p.	Incrementing the proper ballot position registers or counters	Accept	NA	M100 is not a DRE	F, R	Counts successful prints, not votes cast
q.	Protecting the secrecy of the vote throughout the voting process	Accept	NA	M100 is not a DRE	F, R	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
r.	Prohibiting access to voted ballots until after the close of polls	Accept	NA	M100 is not a DRE		No DRE
s.	Provides the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the system	Accept	NA	M100 is not a DRE	F, R	
t.	Isolating test ballots such that they are accounted for accurately in vote counts and are not reflect in official vote counts for specific candidates or measures	Accept	NA	M100 is not a DRE	F, R	VAT has a separate test mode; isolating ballot is procedural
2.5	<b>Post-Voting Functions</b> All systems shall provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails. In additions precinct count systems must provide a means to close the polling place including generating appropriate reports if the system provide the capability to broadcast results, additional standards apply.					
VVSG 2005 2.4	<b>Post Vote Capabilities</b> All systems shall provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails. In additions precinct count systems must provide a means to close the polls including generating appropriate reports if the system provide the capability to broadcast results, additional standards apply					
2.5.1	<b>Closing the Polling Place (Precinct Count)</b> These standards for closing the polls are specific to precinct count systems. The system shall provide the means for:					
VVSG 2005 2.4.1	<b>Closing the Polls</b> These requirements for closing the polls and locking voting systems against future voting are specific to precinct count systems. The voting system shall provide the means for:					
a.	Preventing the further casting of ballots once the polls has closed	Accept	F-M100, R3210		F, R	VAT doesn't close, switched to Off
b. VVSG 2005 b.	Provides an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal	Accept	F-M100, R3210 F-DS200		F, R	
c.	Incorporating a visible indication of system status	Accept	F-M100, R3210		F, R	
d.	Producing a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated	Accept	F-M100, R3210		F, R	
e.	Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election	Accept	F-M100, R3210	M100 reopened with authorization	F, R	DS200 reopened with authorization
2.5.2 VVSG 2005 2.4.2	<b>Consolidating Vote Data</b>					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
	All systems provide a means to consolidate and report vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes).	Accept	F-M100, R3210 F-DS200		F, R	
2.5.3 VVSG 2005 2.4.3	<b>Producing Reports</b>					
	All systems shall be able to create reports summarizing the data on multiple levels.	Accept	F-M100, R3210 F-DS200		F, R	
2.5.3.1	Common Standards All systems shall provide capabilities to:					
a. VVSG 2005 a.	Support of geographic reporting, which requires the reporting of all results for each contest at the precinct level and additional jurisdictional levels	Accept	F-M100, R3210 F-DS200		F, R	
b. VVSG 2005 b.	Produce a printed report of the number of ballots counted by each tabulator	Accept	F-M100, R3210 F-DS200		F, R	
c. VVSG 2005 c.	Produce a printed report for each tabulator of the results of each contest that includes the votes cast for each selection, the count of undervotes, and the count of overvotes	Accept	F-M100, R3210 F-DS200	RFI 2007-06	F, R	RFI 2007-06
d. VVSG 2005 d.	Produce a consolidated printed report of the results for each contest of all votes cast (including the count of ballots from other sources supported by the system as specified by the vendor) that includes the votes cast for each selection, the count of undervotes, and the count of overvotes	Accept	F-M100, R3210 F-DS200	RFI 2007-06	F, R	RFI 2007-06
e. VVSG 2005 e.	Be capable of producing a consolidated printed report of the combination of overvotes for any contest that is selected by an authorized official (e.g.; the number of overvotes in a given contest combining candidate A and candidate B, combining candidate A and candidate C, etc.)	Accept	F-M100, R3210 F-DS200		F, R	
f.	Produce all system audit information required in Section 4.4 in the form of printed reports, or in electronic memory for printing centrally	Accept	F-M100, R3210, F-DS200		F, R	
VVSG 2005 f.	Produce all system audit information required in Section 5.4 in the form of printed reports, or in electronic memory for printing centrally	Accept	F-DS200			
g. VVSG 2005 g.	Prevent data from being altered or destroyed by report generation, or by the transmission of results over telecommunications lines	Accept	F-M100, R3210, F-DS200	Disabled M100 telecommunication in Unity 3.2.1.0 #144- Closed	F, R	Telecommunication is disabled in <b>ESSUNITY3200</b>
2.5.3.2	Precinct Count Systems In addition, all precinct count voting systems shall:					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
a. VVSG 2005 h.	Prevent the printing of reports and the unauthorized extraction of data prior to the official close of the polling place	Accept	F-M100, R3210 F-DS200		F, R	
b. VVSG 2005 i.	Provide a means to extract information from a transportable programmable memory device or data storage medium for vote consolidation	Accept	F-M100, R3210 F-DS200		F, R	
c. VVSG 2005 j.	Consolidate the data contained in each unit into a single report for the polling place when more than one voting machine or precinct tabulator is used	Accept	F-M100, R3210 F-DS200		F, R	
d.	Prevent data in transportable memory from being altered or destroyed by report generation, or by the transmission of results over telecommunications lines	Accept	F-M100, R3210	Disabled M100 telecommunication in Unity 3.2.1.0	F, R	Telecommunication is disabled in <b>ESSUNITY3200</b>
2.5.4	<b>Broadcasting Results</b> Some voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available shall:					
a.	Provide only aggregated results, and not data from individual ballots	Accept	F-M100		F	
b.	Provide no access path from unofficial electronic reports or files to the storage devices for official data	Accept	F-M100		F	
c.	Clearly indicate on each report or file that the results it contains are unofficial	Accept	F-M100		F	
2.6	<b>Maintenance, Transportation and Storage</b> All systems shall be designed and manufactured to facilitate preventive and corrective maintenance, conforming to the hardware standards described in Section 3. All vote casting and tally equipment designated for storage between elections shall: a. Function without degradation in capabilities after transit to and from the place of use, as demonstrated by meeting the performance standards described in Section 3 b. Function without degradation in capabilities after storage between elections, as demonstrated by meeting the performance standards described in Section 3. (See Section 3.2)					Test results are identified in the cross referenced sections
3	<b>Hardware Standards</b>					
3.2	<b>Performance Requirements</b> Performance requirements address a broad range of parameters (see below)					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
3.2.1	<b>Accuracy Requirements</b> Voting system accuracy addresses the accuracy of data for each of the individual ballot positions that could be selected by a voter, including the positions that are not selected. For a voting system, accuracy is defined as the ability of the system to capture, record, store, consolidate and report the specific selections and absence of selections, made by the voter for each ballot position without error. Required accuracy is defined in terms of an error rate that for testing purposes represents the maximum number of errors allowed while processing a specified volume of data.					RFI 2007-06
a. 1) 2)	For all paper-based voting systems: Scanning ballot positions on paper ballots to detect selections for individual candidates and contests Conversion of selections detected on paper ballots into digital data	Accept	F-M100, R3210	Also validated in Volume tests	F, R	
b. 1) 2)	For all DRE voting systems: Recording the voter selections of candidates and contests into voting data storage Recording voter selections of candidates and contests into ballot image storage independently from voting data storage	Accept	NA	M100 is not a DRE	NA	No DRE
c. 1)	For precinct-count voting systems (paper-based and DRE): Consolidation of vote selection data from multiple precinct-based voting machines to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data	Accept	F-M100, R3210		F, R	
d. 1)	For central-count voting systems (paper-based and DRE): Consolidation of vote selection data from multiple counting devices to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data	Accept	F-M100, R3210		F, R	
	For testing purposes, the acceptable error rate is defined using two parameters: the desired error rate to be achieved, and the maximum error rate that should be accepted by the test process. For each processing function indicated above, the voting system shall achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions.	Accept	F-M100		F, V9	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
3.2.2	<b>Environmental Requirements</b> All voting systems shall be designed to withstand the environmental conditions contained in the appropriate test procedures of the Standards/Guidelines. These procedures will be applied to all devices for casting, scanning and counting ballots, except those that constitute COTS devices that have not been modified in any manner to support their use as part of a voting system and that have a documented record of performance under conditions defined in the Standards/Guidelines.			COTs equipment involved with casting, scanning or counting ballots was included in the operating HW during this testing		
	The Technical Data Package supplied by the vendor shall include a statement of all requirements and restrictions regarding environmental protection, electrical service, recommended auxiliary power, telecommunications service, and any other facility or resource required for the proper installation and operation of the system.	Accept	E-M100 E-DS200	PCA HW Doc Review and Operating procedures used to set up for testing	E	
3.2.2.1	<b>Shelter Requirements</b>					
	Precinct count systems are designed for storage and operation in any enclosed facility ordinarily used as a warehouse or polling place, with prominent instructions as to any special storage requirements	Accept	F-M100		F	
3.2.2.2	<b>Space Requirements</b>					
	The arrangement of the voting system does not impede performance of their duties by polling place officials, the orderly flow of voters through the polling place, or the ability for the voter to vote in private	Accept	F-M100		F	
3.2.2.3	<b>Furnishings and Fixtures</b>					
	Any furnishings or fixtures provided as a part of voting systems, and any components provided by the vendor that are not a part of the system but that are used to support its storage, transportation, or operation, comply with the design and safety requirements of Subsection 3.4.8.	Accept	F-M100, E-M100, E-DS200		F, E	
3.2.2.4 <b>VVSG 2005 4.1.2.4</b>	<b>Electrical Supply</b> Components of voting systems that require an electrical supply shall meet the following standards:					
a.	Precinct count systems operate with the electrical supply ordinarily found in polling places (Nominal 120 Vac/60Hz/1 phase)	Accept	E-M100		E	
b.	For components of voting systems that require an electrical supply, central count systems operate with the electrical supply ordinarily found in central tabulation facilities or computer room facilities (120vac/60hz/1, 208vac/60hz/3, or 240vac/60hz/2);	Accept	E-M100		E	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
c. VVSG 2005 c	All voting machines shall also be capable of operating for a period of at least 2 hours on backup power, such that no voting data is lost or corrupted nor normal operations interrupted. When backup power is exhausted the voting machine shall retain the contents of all memories intact. The backup power capability is not required to provide lighting of the voting area.	Accept	E-M100, F-DS200 R-DS200	RFI 2008-02 RFI 2008-06	E	RFI 2008-02 RFI 2008-06
3.2.2.5 VVSG 2005 4.1.2.5	Electrical Power Disturbance Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand, without disruption of normal operation or loss of data:			RFI 2008-02 RFI 2008-06		RFI 2008-02 RFI 2008-06
a.	Surges of 30% dip @10 ms;	Accept	E-M100, E-DS200		E	
b.	Surges of 60% dip @100 ms & 1 sec	Accept	E-M100, E-DS200		E	
c.	Surges of >95% interrupt @5Sec;	Accept	E-M100, E-DS200		E	
d.	Surges of + or - 15% line variations of nominal line voltage	Accept	E-M100, E-DS200		E	
e.	Electric power increases of 7.5% and reductions of 12.5% of nominal specified power supply for a period of up to four hours at each power level.	Accept	E-M100, E-DS200		E	
3.2.2.6 VVSG 2005 4.1.2.6	Electrical Fast Transient Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand, without disruption of normal operation or loss of data, electrical fast transients of:			RFI 2008-10		RFI 2008-10
a.	2 kV AC & DC External Power lines	Accept	E-M100, E-DS200		E	
b.	+ or - 1 kV all external wires > 3 m no control	Accept	E-M100, E-DS200		E	
c.	+ or - 2 kV all external wires control.	Accept	E-M100, E-DS200		E	
3.2.2.7 VVSG 2005 4.1.2.7	Lightning Surge Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand, without disruption of normal operation or loss of data, surges of:					
a.	+ or - 2 kV AC line to line	Accept	E-M100, E-DS200		E	
b.	+ or - 2 kV AC line to earth	Accept	E-M100, E-DS200		E	
c.	+ or - 0.5 kV DC line to line >10m	Accept	E-M100, E-DS200		E	
d.	+ or - 0.5 kV DC line to earth >10m	Accept	E-M100, E-DS200		E	
e.	+ or - 1 kV I/O sig/control >30m	Accept	E-M100, E-DS200		E	
3.2.2.8 VVSG 2005 4.1.2.8	Electrostatic Disruption					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
	The vote scanning and counting equipment for paper-based systems, and all DRE equipment, is able to withstand $\pm 15$ kV air discharge and $\pm 8$ kV contact discharge without damage or loss of data. The equipment may reset or have momentary interruption so long as normal operation is resumed without human intervention or loss of data. Loss of data means votes that have been completed and confirmed to the voter.	Accept	E-M100, E-DS200 NOC 08-001	Reuse of prior testing for the M100	E	
3.2.2.9 <b>VVSG 2005 4.1.2.9</b>	Electromagnetic Radiation					
	Vote scanning and counting equipment for paper-based systems, and all DRE equipment, complies with the Rules and Regulations of the Federal Communications Commission, Part 15, Class B requirements for both radiated and conducted emissions	Accept	E-M100, E-DS200		E	
3.2.2.10 <b>VVSG 2005 4.1.2.10</b>	Electromagnetic Susceptibility					
	Vote scanning and counting equipment for paper-based systems, and all DRE equipment, is able to withstand an electromagnetic field of 10 V/m modulated by a 1 kHz 80% AM modulation over the frequency range of 80 MHz to 1000 MHz, without disruption of normal operation or loss of data	Accept	E-M100, E-DS200		E	
3.2.2.11 <b>VVSG 2005 4.1.2.11</b>	Conducted RF Immunity Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand, without disruption of normal operation or loss of data, conducted RF energy of:					
a.	10V AC & DC power	Accept	E-M100, E-DS200		E	
b.	10V, 20 sig/control >3m.	Accept	E-M100, E-DS200		E	
3.2.2.12 <b>VVSG 2005 4.1.2.12</b>	Magnetic Fields Immunity					
	Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand, without disruption of normal operation or loss of data, AC magnetic fields of 30 A/m at 60 Hz	Accept	E-M100, E-DS200		E	
3.2.2.13	Environmental Control – Operating Environment					
	Equipment used for election management activities or vote counting (including both precinct and central count systems) shall be capable of operation in temperatures ranging from 50 to 95 degrees Fahrenheit.	Accept	E-M100, E-DS200		E	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
3.2.2.14	Environmental Control – Transit and Storage Equipment used for vote casting or for counting votes in a precinct count system, shall meet these specific minimum performance standards that simulate exposure to physical shock and vibration associated with handling and transportation by surface and air common carriers, and to temperature conditions associated with delivery and storage in an uncontrolled warehouse environment:					
a.	High and low storage temperatures ranging from -4 to +140 degrees Fahrenheit, equivalent to MIL-STD-810D, Methods 501.2 and 502.2, Procedure I-Storage;	Accept	E-M100		E	
b.	Bench handling equivalent to the procedure of MIL-STD-810D, Method 516.3, Procedure VI;	Accept	E-M100		E	
c.	Vibration equivalent to the procedure of MIL-STD-810D, Method 514.3, Category 1- Basic Transportation, Common Carrier	Accept	E-M100		E	
d.	Uncontrolled humidity equivalent to the procedure of MIL-STD-810D, Method 507.2, Procedure I-Natural Hot-Humid.	Accept	E-M100		E	
3.2.2.15	Data Network Requirements					
	Voting systems may use a local or remote data network. If such a network is used, then all components of the network shall comply with the telecommunications requirements described in Section 5 and the Security requirements described in Section 6.	Accept	S3210, T3210	Network LAN functionality for the EMS only	S, T	Network functionality is disabled in the submitted voting system
3.2.3	<b>Election Management System (EMS) Requirements</b> The Election Management System (EMS) requirements address electronic hardware and software used to conduct the pre-voting functions defined in Section 2 with regard to ballot preparation, election programming, ballot and program installation, readiness testing, verification at the polling place, and verification at the central location.					
3.2.3.1	Recording Requirements Voting systems shall accurately record all election management data entered by the user, including election officials or their designees.					
a.	Record every entry made by the user;	Accept	F-M100, R3210	Unmodified from <b>ESSUNITY3200</b>	F, R	
b.	Add permissible voter selections correctly to the memory components of the device;	Accept	F-M100, R3210	Unmodified from <b>ESSUNITY3200</b>	F, R	
c.	Verify the correctness of detection of the user selections and the addition of the selections correctly to memory	Accept	F-M100, R3210	Unmodified from <b>ESSUNITY3200</b>	F, R	
d.	Add various forms of data entered directly by the election official or designee, such as text, line art, logos, and images	Accept	F-M100	Unmodified from <b>ESSUNITY3200</b>	F	
e.	Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory	Accept	F-M100, R3210	Unmodified from <b>ESSUNITY3200</b>	F, R	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
f.	Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals	Accept	E-M100		E	
g.	Log corrected data errors by the system.	Accept	F-M100, R3210	Unmodified from <b>ESSUNITY3200</b>	F, R	
3.2.3.2	Memory Stability Memory devices used to retain election management data shall have demonstrated error-free data retention for a period of 22 months.	Accept	Doc Review – Attestation from ESS		TDP	Attestation from ESS
<b>3.2.4</b>	<b>Vote Recording Requirements</b>					
3.2.4.1	Common Standards All voting systems shall provide voting booths or enclosures for poll site use. Such booths or enclosures may be integral to the voting system or supplied as components of the voting system, and shall:					
a.	Be integral to, or make provisions for installation of the voting device;	Accept	F-M100		F	
b.	Ensure by its structure stability against movement or overturning during entry, occupancy, and exit by the voter	Accept	F-M100		F	
c.	Provide privacy for the voter, and be designed in such a way as to prevent observation of the ballot by any person other than the voter	Accept	F-M100		F	
d.	Be capable of meeting the accessibility requirements of Subsection 2.2.7.1	Accept	F-M100		F	
3.2.4.2	Paper-based Recording Standards The paper-based recording requirements govern: <ul style="list-style-type: none"><li>• Ballot cards or sheets, and pages or assemblies of pages containing ballot field identification data</li><li>• Punching devices</li><li>• Marking devices</li><li>• Frames or fixtures to hold the ballot while it is being punched</li><li>• Compartments or booths where voters record selections</li><li>• Secure containers for the collection of voted ballots</li></ul>					
3.2.4.2.1	Paper Ballot Standards Paper ballots used by paper-based voting systems shall meet the following standards:					
a.	Paper ballots used by paper-based voting systems shall meet the following standards: Punches or marks that identify the unique ballot format, in accordance with Section 2.3.1.1.c., shall be outside the area in which votes are recorded, so as to minimize the likelihood that these punches or marks will be mistaken for vote responses and the likelihood that recorded votes will obliterate these punches or marks	Accept	F-M100, R3210	No ballot punches	F, R	No ballot punches

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
b.	If printed or punched alignment marks are used to locate the vote response fields on the ballot, these marks shall be outside the area in which votes are recorded, so as to minimize the likelihood that these marks will be mistaken for vote responses and the likelihood that recorded votes will obliterate these marks	Accept	F-M100, R3210, F-DS200	No ballot punches, ballot and document review	F, R	No ballot punches
c.	The TDP shall specify the required paper stock, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size and location of punch or mark fields used for vote response fields and to identify unique ballot formats, placement of alignment marks, ink for printing, and folding and bleed-through limitations for preparation of ballots that are compatible with the system.	Accept	F-M100		F	
3.2.4.2.2	Punching Devices Punching devices used by voting systems shall:					
a.	Be suitable for the type of ballot card specified;	Accept	NA	Not a punch card system	NA	Not a punch card system
b.	Facilitate the clear and accurate recording of each vote intended by the voter;	Accept	NA	Not a punch card system	NA	Not a punch card system
c.	Be designed to avoid excessive damage to vote recorder components	Accept	NA	Not a punch card system	NA	Not a punch card system
d.	Incorporate features to ensure that chad (debris) is removed, without damage to other parts of the ballot card.	Accept	NA	Not a punch card system	NA	Not a punch card system
3.2.4.2.3	Marking Devices The Technical Data Package shall specify marking devices (such as pens or pencils) that, if used to make the prescribed form of mark, produce readable marked ballots such that the system meets the performance requirements for accuracy specified previously. These specifications shall identify:					
a.	Specific characteristics of marking devices that affect readability of marked ballots	Accept	F-M100		F	
b.	Performance capabilities with regard to each characteristic	Accept	F-M100		F	
c.	For marking devices manufactured by multiple external sources, a listing of sources and model numbers that are compatible with the system.	Accept	F-M100		F	
3.2.4.2.4	Frames or Fixtures for Punchcard Ballots A frame or fixture for punchcard ballot shall:					
a.	Hold the ballot card securely in the proper location and orientation for voting:	Accept	NA	Not a punch card system	NA	Not a punch card system

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
b.	When contests not directly printed on the ballot card or sheet, incorporate an assembly of ballot label pages that identify offices and issues corresponding to the proper ballot format for the polling place where it is used and are aligned with the voting fields assigned to them	Accept	NA	Not a punch card system	NA	Not a punch card system
c.	Incorporate a template to preclude perforation of the card except in the specified voting fields; a mask to allow punches only in fields designated by the format of the ballot; and a backing plate for the capture and removal of chad. The requirement may be satisfied by equipment of a different design as long it achieves the same result as the Standard with regard to:	Accept	NA	Not a punch card system	NA	Not a punch card system
1)	Positioning the card;	Accept	NA	Not a punch card system	NA	Not a punch card system
2)	Association of ballot label information with corresponding punch fields;	Accept	NA	Not a punch card system	NA	Not a punch card system
3)	Enable only those voting fields that correspond to the format of the ballot; and	Accept	NA	Not a punch card system	NA	Not a punch card system
4)	Punching the fields and the positive removal of chad.	Accept	NA	Not a punch card system	NA	Not a punch card system
3.2.4.2.5	Frames or Fixtures for Printed Ballots A frame or fixture for printed ballot cards is optional. If such a device is provided, it shall:					
a.	Be of any size and shape consistent with its intended use;	Accept	NA	No optional frame	F	
b.	Position the card properly;	Accept	NA	No optional frame	F	
c.	Hold the ballot card securely in its proper location and orientation for voting	Accept	NA	No optional frame	F	
d.	Comply with the design and construction requirements in Subsection 3.4.	Accept	NA	No optional frame	F	
3.2.4.2.6	Ballot Boxes and Ballot Transfer Boxes Ballot boxes and ballot transfer boxes which serve as secure containers for the storage and transportation of voted ballots, shall:					
a.	Be of any size, shape, and weight commensurate with their intended use	Accept	F-M100, R3210		F	
b.	Incorporate locks or seals, and specifications in the system documentation	Accept	F-M100, S3210, R3210	M100 v.1:2.2.1	F, S	DS200 v.1:2.2.1
c.	Provide specific points where ballots are inserted, with all other points on the box constructed in a manner that prevents ballot insertion	Accept	F-M100, R3210		F	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
d.	For precinct count systems, contain separate compartments for segregating unread ballots, ballots with write-in votes, or irregularities that may require special handling or processing. In lieu of compartments, conversion processing may mark such ballots with an identifying spot or stripe to facilitate manual segregation	Accept	F-M100, R3210		F	
3.2.4.3	DRE Systems Recording Requirements					
3.2.4.3.1	Activity Indicator DRE systems shall include an audible or visible activity indicator providing the status of each voting device. This indicator shall:					
a.	Indicate whether the device has been activated for voting	Accept	NA	M100 is not a DRE	F, R	VAT prompts to insert a ballot
b.	Indicate whether the device is in use.	Accept	NA	M100 is not a DRE	F, R	
3.2.4.3.2	DRE System Vote Recording To ensure vote recording accuracy and integrity while protecting the anonymity of the voter, all DRE systems shall:					
a.	Contain all mechanical, electromechanical, and electronic components; software; and controls required to detect and record the activation of selections made by the voter in the process of voting and casting a ballot	Accept	NA	M100 is not a DRE	F, R	
b.	Incorporate redundant memories to detect and allow correction of errors caused by the failure of any of the individual memories	Accept	NA	M100 is not a DRE	NA	No DRE
c. 1) 2)	Provide at least two processes that record the voter's selections that: • To the extent possible, are isolated from each other • Designate one process and associated storage location as the main vote detection, interpretation, processing and reporting path	Accept	NA	M100 is not a DRE	NA	No DRE
	Use a different process to store ballot images, for which the method of recording may include any appropriate encoding or data compression procedure consistent with the regeneration of an unequivocal record of the ballot as cast by the voter.	Accept	NA	M100 is not a DRE	NA	No DRE
d.	Provide a capability to retrieve ballot images in a form readable by humans.	Accept	NA	M100 is not a DRE	NA	No DRE
e.	Ensure that all processing and storage protects the anonymity of the voter.	Accept	NA	M100 is not a DRE	F	
3.2.4.3.3	Recording Accuracy DRE systems meet the following requirements for recording accurately each vote and ballot cast:					
a.	Detect every selection made by the voter	Accept	NA	M100 is not a DRE	F, R	
b.	Correctly add permissible selections to the memory components of the device	Accept	NA	M100 is not a DRE	F, R	Temporary memory prior to VAT printing

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
c.	Verify the correctness of the detection of the voter selections and the addition of the selections to memory	Accept	NA	M100 is not a DRE	F, R	
d.	Achieve an error rate not to exceed the requirement indicated in Section 3.2.1	Accept	NA	M100 is not a DRE	F	VAT paper ballot marking
e.	Preserve the integrity of voting data and ballot images (for DRE machines) stored in memory for the official vote count and audit trail purposes against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals	Accept	NA	M100 is not a DRE	NA	No DRE
f.	Maintain a log of corrected data	Accept	NA	M100 is not a DRE	F, R	
3.2.4.3.4	<b>Recording Reliability</b>					
	Recording reliability refers to the ability of the DRE system to record votes accurately at its maximum rated processing volume for a specified period of time. The DRE system shall record votes reliably in accordance with the requirements of Subsection 3.4.3.	Accept	NA	M100 is not a DRE	F	VAT paper ballot marking
3.2.5	<b>Paper-based Conversion Requirements</b>					
3.2.5.1	<b>Ballot Handling</b>					
	Ballot handling consists of a ballot card's acceptance, movement through the read station and transfer into a collection station or receptacle.	Accept	F-M100, R3210		F, R	
3.2.5.1.1	<b>Capacity (Central Count)</b>					
	The capacity to convert the marks on individual ballots into signals is uniquely important to central count systems. The capacity for a central count system shall be documented by the vendor. This documentation shall include capacity for individual components that impact the overall capacity.	Accept	F-M100, R3210	FCA Doc Review	F, R	
3.2.5.1.2	Exception Handling (Central Count) This requirement refers to the handling of ballots when they are unreadable or some condition is detected requiring that the cards be segregated from normally processed ballots for human review. In response to an unreadable ballot or a write-in vote all central count paper-based systems shall central count paper-based systems shall:					
a. b. c.	Outstack the ballot, or Stop the ballot reader and display a message prompting the election official or designee to remove the ballot, or Mark the ballot with an identifying mark to facilitate its later identification.	Accept	R3210	Meets option B	F, R	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
	Additionally, the system shall provide a capability that can be activated by an authorized election official to identify ballots containing overvotes, blank ballots, and ballots containing undervotes in a designated race. If enabled, these capabilities shall perform one of the above actions in response to the indicated condition	Accept	R3210		F, R	
3.2.5.1.3	Exception Handling (Precinct Count) This requirement refers to the handling of ballots for precinct count system when they are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review. All paper based precinct count systems shall:					
VVSG 2005 4.1.5.1.	When ballots are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review (e.g. write-in votes) all precinct count systems shall:					
a. VVSG 2005 i.	In response to an unreadable or blank ballot, return the ballot and provide a message prompting the voter to examine the ballot	Accept	F-M100, R3210 F-DS200		F, R	
b. VVSG 2005 ii.	In response to a ballot with a write-in vote, segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification	Accept	F-M100, R3210 F-DS200		F, R	
c. VVSG 2005 iii. 1) 2) 3) 4) 5)	In response to a ballot with an overvote the system shall: <ul style="list-style-type: none"><li>• Provide a capability to identify an overvoted ballot</li><li>• Return the ballot</li><li>• Provide an indication prompting the voter to examine the ballot</li><li>• Allow the voter to correct the ballot</li><li>• Provide a means for an authorized election official to deactivate this capability entirely and by contest</li></ul>	Accept	F-M100, R3210 F-DS200		F, R	
d. 1) 2) 3) 4) 5)	In response to a ballot with an undervote, the system shall: <ul style="list-style-type: none"><li>• Provide a capability to identify an undervoted ballot</li><li>• Return the ballot</li><li>• Provide an indication prompting the voter to examine the ballot</li><li>• Allow the voter to submit the ballot with the undervote</li><li>• Provide a means for an authorized election official to deactivate this capability</li></ul>	Accept	F-M100, R3210		F, R	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
VVSG 2005 iv.	In response to a ballot with an undervote, the system shall: <ul style="list-style-type: none"><li>• Provide a capability to identify an undervoted ballot</li><li>• Return the ballot</li><li>• Provide an indication prompting the voter to examine the ballot</li><li>• Allow the voter to correct the ballot</li><li>• Allow the voter to submit the ballot with the undervote</li><li>• Provide a means for an authorized election official to deactivate this capability</li></ul>	Accept	F-DS200			
3.2.5.1.4	Multiple Feed Prevention Multiple feed refers to the situation arising when a ballot reader attempts to read more than one ballot at a time. The requirements govern the ability of a ballot reader to prevent multiple feed or to detect and provide an alarm indicating multiple feed.					
a.	If multiple feed is detected, the card reader shall halt in a manner that permits the operator to remove the unread cards causing the error, and reinsert them in the card input hopper	Accept	F-M100		F	
b.	The frequency of multiple feeds with ballots intended for use with the system shall not exceed 1 in 10,000	Accept	F-M100		F	
3.2.5.2	Ballot Reading Accuracy This paper-based system requirement governs the conversion of the physical ballot into electronic data. Reading accuracy for ballot conversion refers to the ability to: <ul style="list-style-type: none"><li>◆ Recognize vote punches or marks, or the absence thereof, for each possible selection on the ballot</li><li>◆ Discriminate between valid punches or marks and extraneous perforations, smudges, and folds</li><li>◆ Convert the vote punches or marks, or the absence thereof, for each possible selection on the ballot into digital signals</li></ul> To ensure accuracy, paper-based systems shall:					
a.	Detect punches or marks that conform to vendor specifications with an error rate not exceeding the requirement indicated in Section 3.2.1	Accept	F-M100, F-DS200, R3210, V-M100 1, 2, 4, 11, 12		F, R V1,2,4, 6-10	
b.	Ignore, and not record, extraneous perforations, smudges, and folds;	Accept	F-M100, R3210		F, R	
c.	Reject ballots that meet all vendor specifications at a rate not to exceed 2 percent.	Accept	F-M100, R3210, V-M100 1, 2, 4, 11, 12		F, R, V1,2,4, 6-10	1 incidence @ DS200 & M650 prompted for maintenance at iBeta
3.2.6	<b>Tabulation Processing Requirements</b>					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
3.2.6.1 <b>VVSG 2005</b> 4.1.6.1	Paper-based Processing Requirements The paper-based processing requirements address all mechanical devices, electromechanical devices, electronic devices and software required to perform the logical and numerical functions of interpreting the electronic image of the voted ballot, and assigning votes to the proper memory registers.					
3.2.6.1.1. <b>VVSG 2005</b> .a	Processing Accuracy Processing accuracy refers to the ability of the system to receive electronic signals produced by punches for punchcard systems and vote marks and timing information for marksense systems; perform logical and numerical operations upon these data; and reproduce the contents of memory when required, without error. Specific requirements are detailed below:					
a.	Processing accuracy shall be measured by vote selection error rate, the ratio of uncorrected vote selection errors to the total number of ballot positions that could be recorded across all ballots when the system is operated at its nominal or design rate of processing	Accept	See 3.2.6.1.1d		See 3.2.6.1.1d	No pass/ fail criteria, definition of processing accuracy measurement only
b. <b>VVSG 2005</b> ii.	The vote selection error rate shall include data that denotes ballot style or precinct as well as data denoting a vote in a specific contest or ballot proposition	Accept	F-M100, R3210 F-DS200		F, R	
c. <b>VVSG 2005</b> iii.	The vote selection error rate shall include all errors from any source	Accept	F-M100, R3210 F-DS200		F, R	
d. <b>VVSG 2005</b> iv.	The vote selection error rate shall not exceed the requirement indicated in Subsection 3.2.1	Accept	F-M100, R3210,V-M100 1, 2, 4, 11, 12		F, R V1,2,4, 6-10	V1,2,6,7,9,10 -DS200
3.2.6.1.2	Paper-based system memory devices, used to retain control programs and data, shall have demonstrated error-free data retention for a period of 22 months under the environmental conditions for operation and non-operation (i.e. storage).	Accept	ESS Attestation	Doc Review	TDP	Attestation
3.2.6.2	DRE System Processing Requirements The DRE voting systems processing requirements address all mechanical devices, electromechanical devices, electronic devices, and software required to process voting data after the polls are closed.					
3.2.6.2.1	Processing Speed DRE voting systems shall meet the following requirements for processing speed:					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
a.	Operate at a speed sufficient to respond to any operator and voter input without perceptible delay (no more than three seconds)	Accept	NA	M100 is not a DRE	F	VAT ballot marking; printing exceeds 3 seconds
b.	if the consolidation of polling place data is done locally, perform this consolidation in a time not to exceed five minutes for each device in the polling place	Accept	NA	M100 is not a DRE	NA	No DRE
3.2.6.2.2	Processing Accuracy Processing accuracy is defined as the ability of the system to process voting data stored in DRE voting devices or in removable memory modules installed in such devices. Processing includes all operations to consolidate voting data after the polls have been closed. DRE voting systems shall:					
a.	Produce reports that are completely consistent, with no discrepancy among reports of voting device data produced at any level	Accept	NA –vote date R3210	No DRE or vote data, VAT audit records only	F, R	
b.	Produce consolidated reports containing absentee, provisional or other voting data that are similarly error-free. Any discrepancy, regardless of source, is resolvable to a procedural error, to the failure of a non-memory device or to an external cause	Accept	NA –vote date R3210	No DRE or vote data, VAT audit records only	F, R	
3.2.6.2.3	Memory Stability					
	DRE system memory devices used to retain control programs and data shall have demonstrated error-free data retention for a period of 22 months. Error-free retention may be achieved by the use of redundant memory elements, provided that the capability for conflict resolution or correction among elements is included.	Accept	NA	M100 is not a DRE	NA	No DRE
3.2.7	<b>Reporting Requirements</b>					
3.2.7.1	Removable Storage Memory					
	All storage media that can be removed from the voting system and transported to another location for readout and report generation, these media shall use devices with demonstrated error-free retention for a period of 22 months under the environmental conditions for operation and non-operation contained in Section 3.2.2. Examples of removable storage media include: programmable read-only memory (PROM), random access memory (RAM) with battery backup, magnetic media or optical media.	Accept	Doc Review		TDP Review	Attestation from ESS
3.2.7.2	Printers All printers used to produce reports of the vote count shall be capable of producing:					
a.	Alphanumeric headers	Accept	F-M100, F-DS200, R3210		F, R	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
b.	Election, office and issue labels	Accept	F-M100, F-DS200, R3210		F, R	
c.	Alphanumeric entries generated as part of the audit record.	Accept	F-M100, F-DS200, R3210		F, R	
3.2.8 VVSG 2005 4.1.8	<b>Vote Data Management Requirements</b> The vote data management requirements for all systems address capabilities that manage, process, and report voting data after the data has been consolidated at the polling place or other jurisdictional levels. These capabilities allow the system to:					
a.	Consolidate voting data from polling place data memory or transfer devices	Accept	F-M100, R3210, F-DS200		F, R	
b.	Report polling place summaries; and	Accept	F-M100, R3210, F-DS200		F, R	
c.	Process absentee ballots, data entered manually, and administrative ballot definition data.	Accept	F-M100, R3210, F-DS200		F, R	
	The requirements address all hardware and software required to generate output reports in the various formats required by the using jurisdiction.	Accept	F-M100, R3210, F-DS200		F, R	
3.2.8.1 VVSG 2005 4.1.8.1	Data File Management All voting systems shall provide the capability to:					
a. VVSG 2005 a.	Integrate voting data files with ballot definition files	Accept	F-M100, R3210 F-DS200		F, R	
b. VVSG 2005 b.	Verify file compatibility.	Accept	F-M100, R3210 F-DS200		F, R	
c. VVSG 2005 c.	Edit and update files as required.	Accept	F-M100, R3210 F-DS200		F, R	
3.2.8.2	<b>Data Report Generation:</b>					
VVSG 2005 4.1.8.2	All voting systems shall include report generators for producing output reports at the device, polling place and summary level, with provisions for administrative and judicial subdivision as required by the using jurisdiction	Accept	F-M100, R3210 F-DS200		F, R	
3.3	<b>Physical Characteristics</b>					
3.3.1	<b>Size</b>					
	There is no numerical limitation on the size of any voting equipment, but the size of each voting machine should be compatible with its intended use and the location at which the equipment is to be used.	Accept	F-M100	RFI 2007-05	F	RFI 2007-05
3.3.2	<b>Weight</b>					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
	There is no numerical limitation on the weight of any voting equipment, but the weight of each voting machine should be compatible with its intended use and the location at which the equipment is to be used.	Accept	F-M100		F	
3.3.3	<b>Transport and Storage of Precinct Systems</b> All precinct voting systems shall:					
a.	Provide a means to safely and easily handle, transport, and install voting equipment, such as wheels or a handle or handles	Accept	F-M100		F	No handling issues noted by iBeta
b. 1) 2)	Be capable of using, or be provided with, a protective enclosure rendering the equipment capable of withstanding: Impact, shock and vibration loads associated with surface and air transportation Stacking loads associated with storage	Accept	F-M100		F	
3.4	<b>Design, Construction, and Maintenance Characteristics</b>					
3.4.1	<b>Materials Process and Parts</b> The approach to system design is unrestricted, and may incorporate any form or variant of technology capable of meeting the voting systems requirements and standards. Precinct count systems shall be designed in accordance with best commercial practice for microcomputers, process controllers, and their peripheral components. Central count voting systems and equipment used in a central tabulating environment shall be designed in accordance with best commercial and industrial practice. All voting systems shall:					
a.	Be designed and constructed so that the frequency of equipment malfunctions and maintenance requirements are reduced to the lowest level consistent with cost constraints.	Accept	F-M100		F	
b.	Include, as part of the accompanying TDP, an approved parts list	Accept	F-M100		F	
c.	Exclude parts or components not included in the approved parts list.	Accept	F-M100		F	
3.4.2	<b>Durability</b>					
	All voting systems shall be designed to withstand normal use without deterioration and without excessive maintenance cost for a period of ten years.	Accept	F-M100, RFI 2008-05 ES&S Attestation		F, TDP Review	RFI 2008-05 RFI 2008-05 ES&S Attestation
3.4.3 VVSG 2005 4.3.3	<b>Reliability</b>					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
	<p>The reliability of voting system devices shall be measured as Mean Time Between Failure (MTBF) for the system submitted for testing. MTBF is defined as the value of the ratio of operating time to the number of failures which have occurred in the specified time interval. A typical system operations scenario consists of approximately 45 hours of equipment operation, consisting of 30 hours of equipment set-up and readiness testing and 15 hours of elections operations. For the purpose of demonstrating compliance with this requirement, a failure is defined as any event which results in either the:</p> <ul style="list-style-type: none"> <li>a. Loss of one or more functions</li> <li>b. Degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds</li> </ul> <p>The MTBF demonstrated during certification testing shall be at least 163 hours.</p>	Incomplete – DS200 only  Accept – Reuse of SysTest Labs Reliability testing	R-DS200  F-M100	Testing for the DS200 Freeze/ Shut Down was halted when # 187 was encountered. RFI 2009-06 (for DS200)	E	M650, DS200, VAT
3.4.4	<p><b>Maintainability</b></p> <p>Maintainability represents the ease with which maintenance actions can be performed based on the design characteristics of equipment and software and the processes the vendor and election officials have in place for preventing failures and for reacting to failures. Maintainability includes the ability of equipment and software to self-diagnose problems and make non-technical election workers aware of a problem. Maintainability addresses all scheduled and unscheduled events, which are performed to:</p> <ul style="list-style-type: none"> <li>• Determine the operational status of the system or a component;</li> <li>• Adjust, align, tune, or service components;</li> <li>• Repair or replace a component having a specified operating life or replacement interval;</li> <li>• Repair or replace a component that exhibits an undesirable predetermined physical condition or performance degradation;</li> <li>• Repair or replace a component that has failed; and</li> <li>• Verify the restoration of a component, or the system, to operational status.</li> </ul> <p>Maintainability shall be determined based on the presence of specific physical attributes that aid system maintenance activities, and the ease with which system maintenance tasks can be performed by the ITA. Although a more quantitative basis for assessing maintainability, such as the mean to repair the system is desirable, the qualification of a system is conducted before it is approved for sale and thus before a broader base of maintenance experience can be obtained.</p>				F	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
3.4.4.1	Physical Attributes The following physical attributes will be examined to assess reliability:  a. Presence of labels and the identification of test points b. Provision of built-in test and diagnostic circuitry or physical indicators of condition c. Presence of labels and alarms related to failures d. Presence of features that allow non-technicians to perform routine maintenance tasks (such as update of the system database)					
3.4.4.2	Additional Attributes The following additional attributes will be examined to assess maintainability:  a. Ease of detecting that equipment has failed by a non-technician b. Ease of diagnosing problems by a trained technician c. Low false alarm rates (i.e., indications of problems that do not exist) d. Ease of access to components for replacement e. Ease with which adjustment and alignment can be performed f. Ease with which database updates can be performed by a non-technician g. Adjust, align, tune or service components					
3.4.5 VVSG 2005 4.3.5	<b>Availability-</b> The availability of a voting system is defined as the probability that the equipment (and supporting software) needed to perform designated voting functions will respond to operational commands and accomplish the function. The voting system shall meet the availability standard for each of the following voting functions:  a. For all paper-based voting systems: 1 Recording voter selections (such as by ballot marking or punch) 2 Scanning the punches or marks on paper ballots and converting them into digital data  b. For all DRE systems, recording and storing voter ballot selections c. For precinct count systems (paper-based and DRE), consolidation of vote selection data from multiple precinct based systems to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data  d. For central-count systems (paper-based and DRE), consolidation of vote selection data from multiple counting devices to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
	<p>System availability is measured as the ratio of the time during which the system is operational (up time) to the total time period of operation (up time plus down time). Inherent availability (<math>A_i</math>) is the fraction of time a system is functional, based upon Mean Time Between Failure (MTBF) and Mean Time To Repair (MTTR), that is: <math>A_i = (MTBF)/(MTBF + MTTR)</math> MTTR is the average time required to perform a corrective maintenance task during periods of system operation. Corrective maintenance task time is active repair time, plus the time attributable to other factors that could lead to logistic or administrative delays, such as travel notification of qualified maintenance personnel and travel time for such personnel to arrive at the appropriate site. Corrective maintenance may consist of substitution of the complete device or one of its components, as in the case of precinct count and some central count systems, or it may consist of on-site repair.</p> <p>The voting system shall achieve at least 99 percent availability during normal operation for the functions indicated above. This standard encompasses for each function the combination of all devices and components that support the function, including their MTTR and MTBF attributes.</p>	Accept	F-M100, R-DS200		F, E	
	Vendors shall specify the typical system configuration that is to be used to assess availability, and any assumptions made with regard to any parameters that impact the MTTR. These factors shall include at a minimum:	Accept	F-M100, R-DS200		F	
a.	Recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation	Accept	F-M100, R-DS200		F	
b.	Recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation. Organizational affiliation (i.e., jurisdiction, vendor) of qualified maintenance personnel	Accept	F-M100, R-DS200		F	
c.	Organizational affiliation (i.e., jurisdiction, vendor) of qualified maintenance personnel	Accept	F-M100, R-DS200		F	
<b>3.4.6</b>	<b>Product Marking</b> All voting systems shall:					
a.	Identify all devices with a permanently affixed nameplate or label containing the name of the manufacturer or vendor, the name of the device, its part or model number, its revision letter, its serial number, and if applicable, its power requirements	Accept	F-M100	#110 - Closed	F	
b.	Display on each device a separate data plate containing a schedule for and list of operations required to service or to perform preventive maintenance	Accept	F-M100		F	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
c.	Display advisory caution and warning instructions to ensure safe operation of the equipment and to avoid exposure to hazardous electrical voltages and moving parts at all locations where operation or exposure may occur	Accept	F-M100		F	
<b>3.4.7</b>	<b>Workmanship</b> To help ensure proper workmanship, all manufacturers of voting systems shall:					
a.	Adopt and adhere to practices and procedures to ensure their products are free from damage or defect that could make them unsatisfactory for their intended purpose	Accept	F-M100		F	
b.	Ensure components provided by external suppliers are free from damage or defect that could make them unsatisfactory for their intended purpose.	Accept	F-M100		F	
<b>3.4.8</b>	<b>Safety</b> All voting systems shall meet the following requirements for safety:					RFI 2008-09
a.	All voting system and their components shall be designed to eliminate hazards to personnel or the equipment itself.	Accept	E-M100		E	
b.	Defects in design and construction that can result in personal injury or equipment damage must be detected and corrected before voting systems and components are placed into service.	Accept	E-M100		E	
c.	Equipment design for personnel safety is equal to or better than the appropriate requirements of the Occupational Safety and Health Act, Code of Federal Regulations, as identified in Title 29, part 1910	Accept	E-M100		E	
<b>3.4.9</b>	<b>Human Engineering- Controls and Displays</b> All voting systems and components shall be designed and constructed so as to simplify and facilitate the functions required , and to eliminate the likelihood of erroneous stimuli and responses on the part of the voter or operator. All voting systems shall meet the following requirements for controls and displays:					
a.	In all systems, controls used by the voter or equipment operator shall be conveniently located, shall use designs consistent with their functions, and shall be clearly labeled. Instruction plates are provided, if necessary to avoid ambiguity or incorrect actuation.	Accept	F-M100		F	
b.	Information or data displays are large enough to be readable by voters and operators with no disabilities and by voters with disabilities consistent with the requirements defined in Section 2.2.7 of the Standards.	Accept	F-M100		F	
c.	Status displays meet the same requirements as data displays, and they shall also follow conventional industrial practice with respect to color:	Accept	F-M100		F	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
1	Green, blue, or white displays shall be used for indications of normal status;	Accept	F-M100		F	
2	Amber indicators shall be used to indicate warnings or marginal status; and	Accept	F-M100		F	
3	Red indicators shall be used to indicate error conditions or equipment states that may result in damage or hazard to personnel; and unless the equipment is designed to halt under conditions of incipient damage or hazard, an audible alarm is also be provided.	Accept	F-M100		F	
d.	Color coding shall be selected so as to assure correct perception by voters and operators with color blindness; and shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element (see Appendix C for suggested references).	Accept	F-M100		F	
e.	The system's display does not use flashing or blinking text objects, or other elements having a flash or blink frequency, greater than 2 Hz and lower than 55 Hz	Accept			F	
<b>4</b>	<b>Software Standards</b>					
<b>4.1.1</b>	<b>Software Sources</b>					RFI 2008-03
<b>4.2</b>	<b>Source Design and Coding Standards</b> The software used by voting systems is selected by the vendor and not prescribed by the Standards. This sections provides standards for voting system software with regard to: <ul style="list-style-type: none"><li>• Selection of programming languages</li><li>• Software integrity</li><li>• Software modularity and programming;</li><li>• Control constructs;</li><li>• Naming conventions;</li><li>• Coding conventions; and</li><li>• Comment conventions.</li></ul>	Accept	Source Code Review	SysTest's M100 source code review was approved for reuse. Requirements 4.2.1 through 4.2.7 are found in <a href="#">Appendix B Unity 3.2.1.0 Source Code Review Results</a> and SysTest's Unity 4.0 report . RFI 2007-02	SysTest Report & Appendix B	SysTest's Unity 4.0 source code review was approved for reuse. Requirements 4.2.1 through 4.2.7 are found in the ESSUNITY3200 test report and SysTest's Unity 4.0 report.
<b>4.3</b>	<b>Data and Document Retention</b> All systems shall:					
a.	Maintain the integrity of voting and audit data during an election, and for at least 22 months thereafter, a time sufficient to resolve most contested elections and support other activities related to the reconstruction and investigation of a contested election	Accept	Doc Review		TDP Review	Attestation from ESS
b.	Protect against the failure of any data input or storage device at a location controlled by the jurisdiction or its contractors, and against any attempt at improper data entry or retrieval	Accept	S3210, V-M100 4		S, V4	
<b>4.4</b>	<b>Audit Record Data</b>					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
	Audit trails are essential to ensure the integrity of a voting system. Operational requirements for audit trails are described in Subsection 2.2.5.2 of the Standards. Audit record data are generated by these procedures. The audit record data in the following subsections are essential to the complete recording of election operations and reporting of the vote tally. This list of audit records may not reflect the design constructs of some systems. Therefore, vendors shall supplement it with information relevant to the operation of their specific systems.	Accept	F-M100, S3210	Audit logs are checked in all system level tests	F, S	Document review
<b>4.4.1</b>	<b>Pre-election Audit Records</b>					
	During election definition and ballot preparation, the system shall audit the preparation of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates. The log shall include:	Accept	F-M100,R3210		F,R	
a.	The allowable number of selections for an office or issue;	Accept	F-M100, R3210		F, R	
b.	The combinations of voting patterns permitted or required by the jurisdiction	Accept	F-M100, R3210		F, R	
c.	The inclusion or exclusion of offices or issues as the result of multiple districting within the polling place	Accept	F-M100, R3210		F, R	
d.	Any other characteristics that may be peculiar to the jurisdiction, the election, or the polling place's location	Accept	F-M100, R3210		F, R	
e.	Manual data maintained by election personnel	Accept	F-M100, R3210		F, R	
f.	Samples of all final ballot formats	Accept	F-M100, R3210		F, R	
g.	Ballot preparation edits listings.	Accept	F-M100, R3210		F, R	
<b>4.4.2</b>	<b>System Readiness Audit Records</b> The following minimum requirements apply to system readiness audit records:					
a.	Prior to the start of ballot counting, a system process shall verify hardware and software status and generate a readiness audit record. This record shall include the identification of the software release, the identification of the election to be processed, and the results of software and hardware diagnostic tests	Accept	F-M100, R3210		F, R	
b.	In the case of systems used at the polling place, the record shall include polling place identification	Accept	F-M100, R3210		F, R	
c.	The ballot interpretation logic shall test and record the correct installation of ballot formats on voting devices	Accept	F-M100, R3210		F, R	
d.	The software shall check and record the status of all data paths and memory locations to be used in vote recording to protect against contamination of voting data	Accept	F-M100, R3210		F, R	
e.	Upon the conclusion of the tests, the software shall provide evidence in the audit record that the test data have been expunged	Accept	F-M100, R3210		F, R	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
f.	If required and provided, the ballot reader and arithmetic-logic unit shall be evaluated for accuracy, and the system shall record the results. It shall allow the processing or simulated processing of sufficient test ballots to provide a statistical estimate of processing accuracy	Accept	F-M100		F	
g. 1) 2) 3) 4)	For systems that use a public network, provide a report of test ballots that includes: Number of ballots sent When each ballot was sent Machine from which each ballot was sent specific votes or selections contained in the ballot	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
<b>4.4.3</b> <b>VSG 5.4.3</b>	<b>In-Process Audit Records</b> In-process audit records document system operations during diagnostic routines and the casting and tallying of ballots. At a minimum, the in-process audit records shall contain:					RFI 2008-07
a.	Machine generated error and exception messages to demonstrate successful recovery. Examples include, but are not necessarily limited to:	Accept	V-M100 1, 2, 4, 5, 11, 12, R-DS200	Code Review v.1:4.2.3e	V1-10	Code review v.1:4.2.3e
1)	The source and disposition of system interrupts resulting in entry into exception handling routines	Accept	V-M100 1, 2, 4, 5, 11, 12, F-M100, R3210, R-DS200		V1-10, F, R	
2)	All messages generated by exception handlers	Accept	V-M100 1, 2, 4, 5, 11, 12, F-M100, R3210, R-DS200		V1-10, F, R	
3)	The identification code and number of occurrences for each hardware and software error or failure	Accept	F-M100, \$, R-DS200		F, R	
4)	Notification of system login or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing	Accept	S3210, R-DS200		S	
5)	Other exception events such as power failures, failure of critical hardware components, data transmission errors or other types of operating anomalies	Accept	S3210, R-DS200		S	
b.	Critical system status messages other than informational messages displayed by the system during the course of normal operations. These items include, but are not limited to:	Accept	F-M100, R3210, S3210, R-DS200	v.2: 3.3.1	F, R, S	v.2: 3.3.1
1)	Diagnostic and status messages upon startup	Accept	F-M100, R3210, R-DS200		F, R	
2)	The “zero totals” check conducted before opening the polling place or counting a precinct centrally	Accept	F-M100, R3210, S3210, R-DS200	v.2: 3.3.1	F, R, S	v.2: 3.3.1
3)	For paper-based systems, the initiation or termination of card reader and communications equipment operation	Accept	F-M100, R3210, R-DS200		F, R	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
4)	For DRE machines at controlled voting locations, the event (and time, if available) of activating and casting each ballot (i.e., each voter's transaction as an event). This data can be compared with the public counter for reconciliation purposes	Accept	NA	M100 is not a DRE	F	VAT ballot printing
c.	Non-critical status messages that are generated by the machine's data quality monitor or by software and hardware condition monitors	Accept	F-M100, R-DS200		F	
d.	System generated log of all normal process activity and system events that require operator intervention, so that each operator access can be monitored and access sequence can be constructed	Accept	F-M100, R3210, S3210, R-DS200	v.2: 3.3.1	F, R, S	v.2: 3.3.1
<b>4.4.4</b>	<b>Vote Tally Data</b> In addition to the audit requirements described above, other election-related data is essential for reporting results to interested parties, the press, and the voting public, and is vital to verifying an accurate count. Voting systems shall meet these reporting requirements by providing software capable of obtaining data concerning various aspects of vote counting and producing printed reports. At a minimum, vote tally data shall include:					
a.	Number of ballots cast, using each ballot configuration, by tabulator, by precinct, and by political subdivision	Accept	F-M100, R3210	#9, #144- Closed	F, R	
b.	Candidate and measure vote totals for each contest, by tabulator	Accept	F-M100, R3210	#9 - Closed	F, R	
c.	The number of ballots read within each precinct and for additional jurisdictional levels, by configuration, including separate totals for each party in primary elections	Accept	F-M100, R3210		F, R	
d.	Separate accumulation of overvotes and undervotes for each contest, by tabulator, precinct and for additional jurisdictional levels (no overvotes would be indicated for DRE voting devices)	Accept	F-M100, R3210		F, R	
e.	For paper-based systems only, the total number of ballots both able to be processed and unable to be processed; and if there are multiple card ballots, the total number of cards read	Accept	F-M100, R3210		F, R	
	For systems that produce an electronic file containing vote tally data, the contents of the file shall include the same minimum data cited above for printed vote tally reports.	Accept	F-M100, R3210		F, R	
<b>4.5</b>	<b>Voter Secrecy on DRE Systems</b> All DRE systems shall ensure vote secrecy by:					
a.	Immediately after the voter chooses to cast his or her ballot, record the voter's selections in the memory to be used for vote counting and audit data (including ballot images), and erase the selections from the display, memory, and all other storage, including all forms of temporary storage	Accept	NA	M100 is not a DRE	S	Post printing on the VAT

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
b.	Immediately after the voter chooses to cancel his or her ballot, erase the selections from the display and all other storage, including buffers and other temporary storage	Accept	NA	M100 is not a DRE	S	Pre-printing on the VAT
5	<b>Telecommunications</b>					
5.2	<b>Design, Construction, and Maintenance Requirement</b>					
	Design, construction, and maintenance requirements for telecommunications represent the operational capability of both system hardware and software. These capabilities shall be considered basic to all data transmissions.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
5.2.1	<b>Accuracy</b>					
	The telecommunications components of all voting systems shall meet the accuracy requirements of 3.4.1.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
5.2.2	<b>Durability</b>					
	The telecommunications components of all voting systems shall meet the Durability requirements of 3.4.2.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
5.2.3	<b>Reliability</b>					
	The telecommunications components of all voting systems shall meet the Reliability requirements of 3.4.3.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
5.2.4	<b>Maintainability</b>					
	The telecommunications components of all voting systems shall meet the maintainability requirements of 3.4.4.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
5.2.5	<b>Availability</b>					
	The telecommunications components of all voting systems shall meet the availability requirements of 3.4.5.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
5.2.6	<b>Integrity</b> For WANs using public telecommunications, boundary definition and implementation shall meet the requirements below.					
a.	Outside service providers and subscribers of such providers shall not be given direct access or control of any resource inside the boundary.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
b.	Voting system administrators shall not require any type of control of resources outside this boundary. Typically, an end point of a telecommunications circuit will be a subscriber termination on a Digital Service Unit/Customer Service Unit although the specific technology configuration may vary. Regardless of the technology used, the boundary point must ensure that everything on the voting system side is locally configured and controlled by the election jurisdiction while everything on the public network side is controlled by an outside service provider.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
c.	The system shall be designed and configured such that it is not vulnerable to a single point of failure in the connection to the public network which could cause total loss of voting capabilities at any polling place.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
5.2.7	<b>Confirmation</b> Confirmation occurs when the system notifies the user of the successful or unsuccessful completion of the data transmission, where successful completion is defined as accurate receipt of the transmitted data. To provide confirmation, the telecommunications components of a voting system shall					
d.	Notify the user of the successful or unsuccessful completion of the data transmission; and	Accept	S3210, T3210	No network transmission; see 2.2.2.1 d & e	S, T	No network transmission; see 2.2.2.1 d & e
e.	In the event of unsuccessful transmission, notify the user of the action to be taken.	Accept	S3210, T3210	No network transmission; see 2.2.2.1 d & e	S, T	No network transmission; see 2.2.2.1 d & e
6	<b>Security Standards</b>					
6.2	<b>Access Controls</b>					
6.2.1	<b>Access Control Policy</b>					
6.2.1.1 <b>VVSG 2005</b> 7.2.1	General Access Control Policy			RFI 2008-03		RFI 2008-03
	Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for:	Accept	S3210		S- Doc Review	
a. <b>VVSG 2005</b> a.	Software access controls;	Accept	S3210		S- Doc Review	
b. <b>VVSG 2005</b> b.	Hardware access controls;	Accept	S3210		S- Doc Review	
c. <b>VVSG 2005</b> c.	Communications;	Accept	S3210	#75 - Closed	S- Doc Review	Networking is disabled

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
d. VVSG 2005 d.	Effective password management;	Accept	S3210	#94 - Closed	S- Doc Review	
e. VVSG 2005 e.	Protection abilities of a particular operating system;	Accept	S3210		S- Doc Review	
f. VVSG 2005 f.	General characteristics of supervisory access privileges;	Accept	S3210		S- Doc Review	
g. VVSG 2005 g.	Segregation of duties; and	Accept	S3210		S- Doc Review	
h. VVSG 2005 h.	Any additional relevant characteristics.	Accept	S3210		S- Doc Review	
6.2.1.2	Individual Access Privileges Voting system vendors shall:					
a. VVSG 2005 7.2.1.2	Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access	Accept	S3210	#75, 80, 81 - Closed	S- Doc Review	
b.	Specify whether an individual's authorization is limited to a specific time, time interval or phase of the voting or counting operations	Accept	S3210		S- Doc Review	
c.	Permit the voter to cast a ballot expeditiously, but preclude voter access to all aspects of the vote counting processes	Accept	F-M100, R3210 S3210		S- Doc Review	
6.2.2 VVSG 7.2.2	<b>Access Control Measures</b> Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access, such as:					
a. VVSG 2005 a.	Use of data and user authorization	Accept	S3210 & R3210 E-M100 V-M100	#53 - Closed	S- Doc & Review	
b. VVSG 2005 b.	Program unit ownership and other regional boundaries	Accept	S3210		S- Doc Review	
c. VVSG 2005 c.	One-end or two-end port protection devices	Accept	S3210		S- Doc Review	
d. VVSG 2005 d.	Security kernels	Accept	S3210-		S- Doc Review	
e. VVSG 2005 e.	Computer-generated password keys	Accept	S3210		S- Doc & Code Review	
f. VVSG 2005 f.	Special protocols	Accept	S3210	#53 – Closed	S- Doc Review	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
g. VVSG 2005 g.	Message encryption and	Accept	S3210		S- Doc & Code Review	
h. VVSG 2005 h.	Controlled access security.	Accept	S3210		S- Doc Review	
	Vendors also shall define and provide a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself.	Accept	S3210		S- Doc Review	
6.3. VVSG 2005 7.3	<b>Physical Security Measures</b>					
	A voting system's sensitivity to disruption or corruption of data depends, in part, on the physical location of equipment and data media, and on the establishment of secure telecommunications among various locations. Most often, the disruption of voting and vote counting results from a physical violation of one or more areas of the system thought to be protected. Therefore, security procedures shall address physical threats and the corresponding means to defeat them.	Accept	S3210		S- Doc Review	
6.3.1 VVSG 7.3.1	<b>Polling Place Security</b> For polling place operations, vendors shall develop and provide detailed documentation of measures anticipate and counteract vandalism, civil disobedience, and similar occurrences. The measures shall.					
a. VVSG 2005 a.	Allow the immediate detection of tampering with vote casting devices and precinct ballot counters.	Accept	S3210		S- Doc Review	
b. VVSG 2005 b.	Control physical access to a telecommunications link if such a link is used	Accept	S3210		S- Doc Review	
6.3.2	<b>Central Count Location Security</b>					
VVSG 2005 7.3.2	Vendors shall develop and document in detailed measures to be taken in a central counting environment. These measures shall include physical and procedural controls related to the Handling of ballot boxes Preparing of ballots for counting Counting operations and Reporting data	Accept	S3210		S- Doc Review	
6.4	<b>Software Security</b>					
6.4.1 VVSG 2005 7.4.1	<b>Software and Firmware Installation</b> The system shall meet the following requirements for installation of software, including hardware with embedded firmware.					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
a. VVSG 2005 a.	If software is resident in the system as firmware, the vendor shall require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations.	Accept	S3210	#54 Closed	S- Doc Review	
b. VVSG 2005 b.	To prevent alteration of executable code, no software shall be permanently installed or resident in the voting system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.	Accept	S3210	#54 Closed	S	
c. VVSG 2005 c.	The voting system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote counting program, and its associated exception handlers.	Accept	S3210	#53 Closed	S	
d. VVSG 2005 d.	The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.	Accept	S3210		S	
e. VVSG 2005 e.	After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible.	Accept	S3210		S	
6.4.2 VVSG 2005 7.4.2	<b>Protection Against Malicious Software</b> Voting systems shall deploy protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs					
	Vendors shall develop and document the procedures to be followed to ensure that such protection is maintained in a current status.	Accept	S3210, T3210		S	
6.5	<b>Telecommunications and Data Transmission</b>					
6.5.1	<b>Access Controls</b>					
	Voting systems that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software, and data function.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
6.5.2	<b>Data Integrity</b>					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
	Voting systems that use electrical or optical transmission of data shall ensure the receipt of valid vote records is verified at the receiving station. This should include standard transmission error detection and correction methods such as checksums or message digest hashes. Verification of correct transmission shall occur at the voting system application level and ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot.	Accept	S3210, T3210	No transmission within the polls prior to voter casting their ballot	S, T	No transmission within the polls prior to voter casting their ballot
6.5.3	<b>Data Interception Prevention</b> Voting systems that use telecommunications to communicate between system components and locations before the polling place is officially closed shall:					
a.	Implement an encryption standard currently documented and validated for use by an agency of the U.S. Federal Government and	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
b.	Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
6.5.4	<b>Protection Against External Threats</b>					
	Voting systems that use public telecommunications networks shall implement protections against external threats to which commercial products used in the system may be susceptible.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
6.5.4.1	<b>Identification of COTS Products</b>					
a. b. c. d.	Voting systems that use public telecommunications networks shall provide system documentation that clearly identifies all COTS hardware and software products and communications services used in the development and/or operation of the voting system, including operating systems, communications routers, modem drivers and dial-up networking software.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
	Such documentation shall identify the name, vendor, and version used for each such component.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
6.5.4.2	<b>Use of Protective Software</b>					
	Voting systems that use public telecommunications networks shall use protective software at the receiving-end of all communications paths to:	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
a.	Detect the presence of a threat in a transmission	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
b.	Remove the threat from infected files/data	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
c.	Prevent against storage of the threat anywhere on the receiving device	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
d.	Provide the capability to confirm that no threats are stored in system memory and in connected storage media	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
e.	Provide data to the system audit log indicating the detection of a threat and the processing performed	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
	Vendors shall use multiple forms of protective software as needed to provide capabilities for the full range of products used by the voting system.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
6.5.4.3	<u>Monitoring and Responding to External Threats</u>					
	Voting system that use public telecommunications networks may become vulnerable, by virtue of their system components, to external threats to the accuracy and integrity of vote recording, vote counting, and vote consolidation and reporting processes. Therefore, vendors of such systems shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the vendor will use to:	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
a.	Monitor threats, such as through the review of assessments, advisories, and alerts for COTS components issued by the Computer Emergency Response Team (CERT), for which a current listing can be found at <a href="http://www.cert.org">http://www.cert.org</a> , the National Infrastructure Protection Center (NIPC), and the Federal Computer Incident Response Capability (FedCIRC), for which additional information can be found at <a href="http://www.uscert.gov">www.uscert.gov</a>	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
b.	Evaluate the threats and, if any, proposed responses	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
c.	Develop responsive updates to the system and/or corrective procedures	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
d.	Submit the proposed response to the test labs and appropriate states for approval, identifying the exact changes and whether or not they are temporary or permanent	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
e.	After implementation of the proposed response is approved by the state, assist clients, either directly or through detailed written procedures, how to update their systems and/or to implement the corrective procedures within the timeframe established by the state	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
f.	Address threats emerging too late to correct the system by:	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
1	Providing prompt, emergency notification to the accredited test labs and the affected states and user jurisdictions	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
2	Assisting client jurisdictions directly or advising them through detailed written procedures to disable the public telecommunications mode of the system	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
3	Modifying the system after the election to address the threat, submitting the modified system to an accredited test lab and the EAC or state certification authority for approval, and assisting client jurisdictions directly or advising them through detailed written procedures, to update their systems and/or to implement the corrective procedures after approval	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
6.5.5	<b>Shared Operating Environment</b> Ballot recording and vote counting can be performed in either a dedicated or non-dedicated environment. If ballot recording and vote counting operations are performed in an environment that is shared with other data processing functions, both hardware and software features shall be present to protect the integrity of vote counting and of vote data. Systems that use a shared operating environment shall:					
a.	Use security procedures and logging records to control access to system functions	Accept	S3210, T3210	EMS LAN #92 - Closed	S	Telecommunication is disabled in <b>ESSUNITY3200</b>
b.	Partition or compartmentalize voting system functions from other concurrent functions at least logically, and preferably physically as well	Accept	S3210, T3210	EMS LAN	S	Telecommunication is disabled in <b>ESSUNITY3200</b>
c.	Control system access by means of passwords, and restrict account access to necessary functions only	Accept	S3210, T3210	EMS LAN	S	Telecommunication is disabled in <b>ESSUNITY3200</b>
d.	Have capabilities in place to control the flow of information, precluding data leakage through shared system resources	Accept	S3210, T3210	EMS LAN #92 - Closed	S	Telecommunication is disabled in <b>ESSUNITY3200</b>

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
6.5.6	<b>Access to Incomplete Election Returns and Interactive Queries</b> If the voting system provides access to incomplete election returns and interactive inquiries before the completion of the official count, the system shall:					
a.	Be designed to provide external access to incomplete election returns (for equipment that operates in a central counting environment), only if that access for these purposes is authorized by the statutes and regulations of the using agency. This requirement applies as well to polling place equipment that contains a removable memory module or that may be removed in its entirety to a central place for the consolidation of polling place returns	Accept	S3210	No access to incomplete returns #25 - Closed	S	No access to incomplete returns
b.	Design voting system software and its security environment such that data accessible to interactive queries resides in an external file or database created and maintained by the elections software under the restrictions applying to any other output report:	Accept	S3210	No external access #25 - Closed #103- Closed	S	No external access
1	The output file or database has no provision for write-access back to the system.	Accept	S3210	No write back provision #25 - Closed #103- Closed #174 - Closed	S	No write back provision
2	Persons whose only authorized access is to the file or database are denied write-access, both to the file or database, and to the system.	Accept	S3210	No external access #25 - Closed #103- Closed	S	No external access
6.6	<b>Security for Transmission of Official Data Over Public Communications Networks</b>					
6.6.1	<b>General Security Requirements for Systems Transmitting Data Over Public Networks</b> All systems that transmit data over public telecommunications networks shall:					
a.	Preserve the secrecy of voter ballot selections and prevent anyone from violating ballot privacy	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
b.	Employ digital signatures for all communications between the vote server and other devices that communicate with the server over the network	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
c.	Require that at least two authorized election officials activate any critical operation regarding the processing of ballots transmitted over a public communications network, i.e. the passwords or cryptographic keys of at least two employees are required to perform processing of vote	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
6.6.2	<b>Voting Process Security for Casting Individual Ballots over a Public Telecommunications Network</b>					
	Systems designed for transmission of telecommunications over public networks shall meet security standards that address the security risks attendant with the casting of ballots from polling places controlled by election officials using voting devices configured and installed by election officials and/or their vendor or contractor, and using in-person authentication of individual voters.	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
6.6.2.1	Documentation of Mandatory Security Activities Vendors of voting systems that cast individual ballots over a public telecommunications network shall provide detailed descriptions of:					
a.	All activities mandatory to ensuring effective voting system security to be performed in setting up the system for operation, including testing of security before an election	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
b.	All activities that should be prohibited during voting equipment setup and during the time-frame for voting operations, including both the hours when polls are open and when polls are closed	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
6.6.2.2	Capabilities to Operate During Interruption of Telecommunications Capabilities These systems shall provide the following capabilities to provide resistance to interruptions of telecommunications service that prevent voting devices at the polling place from communicating with external components via telecommunications:					
a.	Detect the occurrence of a telecommunications interruption at the polling place and switch to an alternative mode of operation that is not dependent on the connection between polling place voting devices and external system components	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
b.	Provide an alternate mode of operation that includes the functionality of a conventional electronic voting system without losing any single vote	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
c.	Create and preserve an audit trail of every vote cast during the period of interrupted communication and system operation in conventional electronic voting system mode	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
d.	Upon reestablishment of communications, transmit and process votes accumulated while operating in conventional electronic voting system mode with all security safeguards in effect	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
e.	Ensure that all safeguards related to voter identification and authentication are not affected by the procedures employed by the system to counteract potential interruptions of telecommunications capabilities	Accept	S3210, T3210	Disabled M100 telecommunication in Unity 3.2.1.0	S, T	Telecommunication is disabled in <b>ESSUNITY3200</b>
7	<b>Quality Assurance Requirements</b>					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
7.2	<b>General Requirements</b> The voting system vendor is responsible for designing and implementing a quality assurance program to ensure that the design, workmanship, and performance requirements of this standard are achieved in all delivered systems and components. At a minimum, this program shall:					
a.	Include procedures for specifying, procuring, inspecting, accepting, and controlling parts and raw materials of the requisite quality.	Accept	PCA Doc Review Check-in Procedure QA Spot Checklist		F	
b.	Require the documentation of the hardware and software development process.	Accept	PCA Doc Review Check-in Procedure QA Spot Checklist		F	
c.	Identify and enforce all requirements for:	Accept	PCA Doc Review Check-in Procedure QA Spot Checklist		F	
c. 1)	In-process inspection and testing that the manufacturer deems necessary to ensure proper fabrication and assembly of hardware.	Accept	PCA Doc Review Check-in Procedure QA Spot Checklist		F	
c. 2)	Installation and operation of software (including firmware).	Accept	PCA Doc Review Check-in Procedure QA Spot Checklist		F	
d.	Include the plans and procedures for post-production environmental screening and acceptance testing.	Accept	PCA Doc Review Check-in Procedure QA Spot Checklist		F	
e.	Include a procedure for maintaining all data and records required to document and verify the quality inspections and tests.	Accept	PCA Doc Review Check-in Procedure QA Spot Checklist		F	
7.3	<b>Components from Third Parties</b>					
	A vendor who does not manufacture all the components of its voting system, but instead procures components as standard commercial items for assembly and integration into a voting system, shall verify that the supplier vendors follow documented quality assurance procedures that are at least as stringent as those used internally by the voting system vendor.	Accept	PCA Doc Review QA Spot Checklist	#179 & 180 – Informational Closed	F	

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
7.4	<b>Responsibility for Tests</b> The manufacturer or vendor shall be responsible for: a. Performing all quality assurance tests. b. Acquiring and documenting test data. c. 2002: Providing test reports for review by the ITA, and to the purchaser upon request.					
		Accept	PCA Doc Review QA Spot Checklist		F	
		Accept	PCA Doc Review QA Spot Checklist		F	
		Accept	PCA Doc Review QA Spot Checklist		F	
7.5	<b>Parts and Materials Special Tests</b> In order to ensure that voting system parts and materials function properly, vendors shall: a. Select parts and materials to be used in voting systems and components according to their suitability for the intended application. Suitability may be determined by similarity of this application to existing standard practice, or by means of special tests. b. Design special tests, if needed, to evaluate the part or material under conditions accurately simulating the actual operating environment. c. Maintain the resulting test data as part of the quality assurance program documentation.					
		Accept	PCA Doc Review QA Spot Checklist		F	
		Accept	PCA Doc Review QA Spot Checklist		F	
		Accept	PCA Doc Review QA Spot Checklist		F	
7.6	<b>Parts and Materials Special Tests</b> The vendor performs conformance inspections to ensure the overall quality of the voting system and components delivered to the ITA for testing and to the jurisdiction for implementation. To meet the conformance inspection requirements the vendor or manufacturer shall:: a. Inspect and test each voting system or component to verify that it meets all inspection and test requirements for the system. b. Deliver a record of tests or a certificate of satisfactory completion with each system or component.					
		Accept	PCA Doc Review QA Spot Checklist Observe ESS tech perform maint.		F	
		Accept	PCA Doc Review QA Spot Checklist Observe ESS tech perform maint.		F	
7.7	<b>Documentation</b> Vendors are required to produce documentation to support the development and formal testing of voting systems. To meet documentation requirements, vendors shall provide complete product documentation with each voting systems or components, as described Volume II, Section 2 for the TDP. This documentation shall:					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
a.	Be sufficient to serve the needs of the ITA, voters, election officials, and maintenance technicians;	Accept	PCA Doc Review	#85, 113, 126, 127 - Closed	F	Letter of reuse; Appendix C for LogMonitor
b.	Be prepared and published in accordance with standard industrial practice for information technology and electronic and mechanical equipment; and					
c	Consist, at a minimum, of the following: 1) System overview; 2) System functionality description; 3) System hardware specification; 4) Software design and specifications; 5) System security specification; 6) System test and verification specification; 7) System operations procedures;					
<b>8</b>	<b>Configuration Management</b>					
<b>8.1</b>	<b>Scope</b>					
<b>8.1.1</b>	<b>Configuration Management Requirements</b> Configuration management addresses a broad set of record keeping, audit, and reporting activities that contribute to full knowledge and control of a system and its components. These activities include:					
	▪ Identifying discrete system components.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
	▪ Creating records of a formal baseline and later versions of components.	Accept	PCA Doc Review Check-in Procedure	Reuse - Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review Inconsistencies in CM observed in testing were noted #143 & 160
	▪ Controlling changes made to the system and its components.	Accept	PCA Doc Review Check-in Procedure	Reuse - Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review Inconsistencies in CM observed in testing were noted #143 & 160
	▪ Releasing new versions of the system to ITAs.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review Inconsistencies in CM observed in testing were noted #143 & 160

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
	▪ Releasing new versions of the system to customers.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
	▪ Auditing the system, including its documentation, against configuration management records.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
	▪ Controlling interfaces to other systems.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
	▪ Identifying tools used to build and maintain the system.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
<b>8.1.2</b>	<b>Organization of Configuration Management Standards</b>					
<b>8.1.3</b>	Application of Configuration Management Standards Requirements for configuration management apply regardless of the specific technologies employed to all voting systems subject to the Standards. These system components include:					
a.	Software components.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
b.	Hardware components.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
c.	Communications components.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
d.	Documentation.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
e.	Identification and naming and conventions (including changes to these conventions) for software programs and data files.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
f.	Development and testing artifacts such as test data and scripts.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
g.	File archiving and data repositories.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
<b>8.2</b>	<b>Configuration Management Policy</b> The vendor shall describe its policies for configuration management in the TDP. This description shall address the following elements					

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
a.	Scope and nature configuration management program activities.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
b.	Breadth of the application of the vendor's policies and practices to the voting system. (i.e. extent to which policies and practices apply to the total system and extent to which polices and practices of suppliers apply to particular components, subsystems, or other defined system elements.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
<b>8.3</b>	<b>Configuration Identification</b>					
<b>8.3.1</b>	<b>Structuring and Naming Configuration Items</b> The vendor shall describe the procedures and conventions used to:					
a.	Classify configuration items into categories and subcategories.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
b.	Uniquely number or otherwise identify configuration items.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
c.	Name configuration items.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
<b>8.3.2</b>	<b>Version Conventions</b> When a system component is used to identify higher-level system elements, a vendor shall describe the conventions used to:					
a.	Identify the specific versions of individual configuration items and sets of items that are used by the vendor to identify higher level system elements such as subsystems.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
b.	Uniquely number or otherwise identify versions.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
c.	Name versions.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
<b>8.4</b>	<b>Baseline, Promotion and Demotion Procedures</b> The vendor shall establish formal procedures and conventions for establishing and providing a complete description of the procedures and related conventions used to:					
a.	Establish a particular instance of a component as the starting baseline.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
b.	Promote subsequent instances of a component to baseline status as development progresses through to completion of the initial completed version released to the ITAs for qualification testing.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
c.	Promote subsequent instances of a component to baseline status as the component is maintained throughout its life cycle until system retirement (i.e., the system is no longer sold or maintained by the vendor).	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
8.5	<b>Configuration Control Procedures</b> Configuration control is the process of approving and implementing changes to a configuration item to prevent unauthorized additions, changes, or deletions. The vendor shall establish such procedures and related conventions, providing a complete description of those procedures used to:					
a.	Develop and maintain internally developed items.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b> #87, 97, 151, 152, 155 - Closed	F	Letter of Reuse PCA Document Review
b.	Acquire and maintain third-party items.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
c.	Resolve internally identified defects for items regardless of their origin.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
d.	Resolve externally identified and reported defects (i.e., by customers and ITAs).	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
8.6	<b>Release Process Procedures</b> The release process is the means by which the vendor installs, transfers, or migrates the system to the ITAs and, eventually, to its customers. The vendor shall establish such procedures and related conventions, providing a complete description of those used to:		PCA Doc Review Check-in Procedure			
a.	Perform a first release of the system to:	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
b.	Perform a subsequent maintenance or upgrade release of the system, or a particular components, to:	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
c.	Perform the initial delivery and installation of the system to a customer, including confirmation that the installed version of the system matches exactly the certified system version.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
d.	Perform a subsequent maintenance or upgrade release of the system, or a particular component, to a customer, including confirmation that the installed version of the system matches exactly the qualified system version.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
8.7	<b>Configuration Audits</b>					
8.7.1	<b>Physical Configuration Audit</b> The PCA is conducted by the ITA to compare the voting system components submitted for qualification to the vendor's technical documentation. For the PCA, a vendor shall provide:					
a.	Identification of all items that are to be a part of the software release.	Accept	PCA Doc Review Check-in Procedure	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
b.	Specification of compiler (or choice of compilers) to be used to generate executable programs.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
c.	Identification of all hardware that interfaces with the software.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
d.	Configuration baseline data for all hardware that is unique to the system.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
e.	Copies of all software documentation intended for distribution to users, including program listings, specifications, operations manual, voter manual, and maintenance manual.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
f.	User acceptance test procedures and acceptance criteria.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
g.	Identification of any changes between the physical configuration of the system submitted for the PCA and that submitted for the FCA, with a certification that any differences do not degrade the functional characteristics.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
h.	Complete descriptions of its procedures and related conventions used to support this audit by:	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
h. 1)	Establishing a configuration baseline of the software and hardware to be tested.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
h. 2)	Confirming whether the system documentation matches the corresponding system components.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b> #98 - Closed	F	Letter of Reuse PCA Document Review
8.7.2	<b>Functional Configuration Audits</b> The FCA is conducted by the ITA to verify that the system performs all the functions described in the system documentation. The vendor shall:					
a.	Completely describe its procedures and related conventions used to support this audit for all system components.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
b.	Provide the following information to support this audit:	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review

VSS 2002	Certification Test Requirements:	Test Results	Unity 3.2.1.0	Comment	UNITY 3200	Comment
b. 1)	Copies of all procedures used for module or unit testing, integration testing, and system testing.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
b. 2)	Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
b. 3)	Records of all tests performed by the procedures listed above, including error corrections and retests.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
	In addition to such audits performed by ITAs during the system qualification process, elements of this audit may also be performed by state election organizations during the system certification process, and individual jurisdictions during system acceptance testing.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
8.8	<b>Configuration Management Resources</b> Often, configuration management activities are performed with the aid of automated tools. Assuring that such tools are available throughout the system life cycle, including if the vendor is acquired by or merged with another organization, is critical to effective configuration management. Vendors may choose the specific tools they use to perform the record keeping, audit, and reporting activities of the configuration management standards. The resources documentation standard provided below focus on assuring that procedures are in place to record information about the tools to help ensure that they, and the data they contain, can be transferred effectively and promptly to a third party should the need arise. Within this context, a vendor is required to develop and provide a complete description of the procedures and related practices for maintaining information about:					
a.	Specific tools used, current version, and operating environment specifications.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
b.	Physical location of the tools, including designation of computer directories and files.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review
c.	Procedures and training materials for using the tools.	Accept	PCA Doc Review	Unmodified from <b>ESSUNITY3200</b>	F	Letter of Reuse PCA Document Review

## 7.2 Appendix B: PCA Source Code Review

The Unity 3.2.1.0 source code is made up of three parts that required diverse handling based upon the rules of the EAC Certification Program.

The first part is the M100, originally submitted for certification in the Unity 4.0.0.0 certification effort submitted to SysTest. PCA Source Code Review of the M100 v.5.4.0.027 was performed by Sys Test to the VSS 2002. ES&S petitioned the EAC for reuse. The terms of the reuse are identified in the *EAC approval letter 8-04-09 Ltr to ESS reuse of testing*. Any changes from the M100 code provided by SysTest was 100% reviewed by iBeta to the VSS 2002.

The second part is source code that remained unchanged from the **ESSUNITY3200** certification that did not require any additional review or a new Trusted Build. The builds of the unchanged applications were moved into the Unity 3.2.1.0 from the escrow of the prior certification.

The third part is source code that was changed from the **ESSUNITY3200** certification. iBeta conducted a 100% review of source code changes that were either submitted by ES&S in their Unity 3.2.1.0 application or resulted from issues identified during testing. These were reviewed to the VVSG 2005 and are identified in [Section 5.1 PCA Source Code Review](#).

### 7.2.1 Reused Sys Test Source Code Review Results

The results of the M100 source code review conducted by SysTest are addressed in the summary report of the testing performed by SysTest.

### 7.2.2 iBeta Unity 3.2.1.0 Source Code Review Results

The first table below contains the number of discrepancies identified in the 3% review of the M100 code received from SysTest, changes to the M100 code reviewed for Unity 4.0.0.0 and DS200, Scanner\_C8051 ,ERM, HPM, MYDLL, AIMS and VAT changes from the **ESSUNITY3200** escrow. It identifies the final code version reviewed and used in the Trusted Builds performed by iBeta. (See [Appendix G: Trusted Build](#).)

The second table lists the source code review requirements and the discrepancies identified by language. All discrepancies were comment related. These were reported to ES&S. ES&S fixed them and re-submitted them to iBeta. A subsequent review found all comments were appropriately updated. The discrepancies were closed.

Source Code	Language	M100 3% Review for Reuse	Changes to M100 - VSS 2002	Changes to Unity 3.2.0.0 - VVSG 2005	Unity 3.2.1.0 Release Version	Number of Discrepancies
ERM	Cobol	N/A	N/A	7.5.7.0c	7.5.7.0	13
M100	C	5.4.0.0.27	5.4.4.4.1	N/A	5.4.4.4	0 = 3 % review 3 = 100% review
DS200	C/C++	N/A	N/A	1.4.3.7a	1.4.3.7	31
HPM	Cobol	N/A	N/A	5.7.3.0b	5.7.3.0	0
VAT	VB.Net	N/A	N/A	1.3.2907a	1.3.2907	1
AIMS	C#,C/C++, VB,SQL	N/A	N/A	1.3.257	1.3.257	0
MYDLL	C	N/A	N/A	1.1.0.2c	1.1.0.2	11
Scanner_C8051	C	N/A	N/A	2.20.0.0a	2.20.0.0	0

The PCA Source Code Review was conducted against these VSS 2002 and VVSG 2005 requirements. Comment related requirements are highlight in green.

VVSG	VSS	Requirement	Definition	C & C++	Cobol	VB.Net
<b>Vol. 1 Section 4.2.2-Integrity</b>						
v.1: 5.2.2	v.1: 4.2.2	Self-modifying code	Self-modifying, dynamically loaded, or modification of compiled or interpreted code is prohibited	0	0	0
<b>Vol. 1 Section 4.2.3- Modularity</b>						
v.1: 5.2.3.a	v.1: 4.2.3.a	Specific function	Module performs a specific function	1	0	0
v.1: 5.2.3.b	v.1: 4.2.3.b	Module has unique name	Uniquely and mnemonically named using names that differ by more than a single	0	0	0

VVSG	VSS	Requirement	Definition	C & C++	Cobol	VB.Net
			character			
v.1: 5.2.3.b 5.2.7 (a, a.1-a.6)	v.1: 4.2.3.b 4.2.7 (a, a.1-a.6)	<b>Module has header</b>	Header describes purpose, other units needed, inputs, outputs, files read or written, globals, revision records (for modules greater than 10 lines) Header comments shall provide the following information: 1) The purpose of the unit and how it works; 2) Other units called and the calling sequence 3) A description of input parameters and outputs 4) File references by name and method of access 5) Global variables used 6) Date of creation and a revision record	25	0	1
v.1: 5.2.3.c	v.1: 4.2.3.c	<b>Required resources</b>	All required resources, such as data accessed by the module, should either be contained within the module or explicitly identified	0	0	0
v.1: 5.2.3.e	v.1: 4.2.3.e	<b>Single Entry Point</b>	Module has a single entry point	0	0	0
v.1: 5.2.3.e	v.1: 4.2.3.e	<b>Single Exit Point</b>	Module has a single exit point	0	0	0
v.1: 5.2.3.f	v.1: 4.2.3.f	<b>Control structures</b>	Support the modular concept and apply to any language feature where program control passes from one activity to the next.	0	0	0
<b>Vol. 1 Section 4.2.4-Control Constructs</b>						
v.1: 5.2.4.a	v.1: 4.2.4.a	<b>Acceptable Constructs</b>	Acceptable constructs are Sequence, If-Then-Else, Do-While, Do-Until, Case, and the General loop (including the special case for loop);	0	0	0
v.1: 5.2.4.b	v.1: 4.2.4.b	<b>Vendor Defined Constructs with Justification</b>	If the programming language used does not provide these control constructs, the vendor shall provide them (that is, comparable control structure logic). The constructs shall be used consistently throughout the code. No other constructs shall be used to control program logic and execution	0	0	0
v.1: 5.2.4.c	v.1: 4.2.4.c	<b>Execution through Control Constructs</b>	While some programming languages do not create programs as linear processes, stepping from an initial condition, through changes, to a conclusion, the program components nonetheless contain procedures (such as "methods" in object-oriented languages). Even in these programming languages, the procedures must execute through these control constructs.	0	0	0
v.1: 5.2.4.d	v.1: 4.2.4.d	<b>Program re-direction</b>	Logic that evaluates received or stored data shall not re-direct program control	0	0	0
<b>Vol. 1 Section 4.2.5-Naming Conventions</b>						
v.1: 5.2.5.a	v1: 4.2.5.a	<b>Name Readability</b>	Names shall be selected so that their parts of speech represent their use.	4	0	0
v.1: 5.2.5.b 5.2.5.c	v.1: 4.2.5.b 4.2.5.c	<b>Class, function and variable names</b>	Consistent names are used. Names shall be unique within an application and differ by more than a single character.	0	0	0
v.1: 5.2.5.d	v.1: 4.2.5.d	<b>Keyword</b>	Keywords shall not be used as names of objects, functions, procedures, or variables	0	0	0

VVSG	VSS	Requirement	Definition	C & C++	Cobol	VB.Net
<b>Vol. 1 Section 4.2.6-Coding Conventions</b>						
v.2: 5.4.2.a	v.2: 5.4.2.a	<b>Uniform calling sequences</b>	Uses uniform calling sequences.	0	0	0
v.2: 5.4.2.a	v.2: 5.4.2.a	<b>Parameters type and range validation</b>	All parameters shall either be validated for type and range on entry into each unit or the unit comments shall explicitly identify the types and ranges	1	0	0
v.2: 5.4.2.b	v.2: 5.4.2.b	<b>Explicit return values</b>	The return is explicitly defined for functions and explicitly assigned	0	0	0
v.2: 5.4.2.c	v.2: 5.4.2.c	<b>Macros</b>	Does not use macros that contain returns or pass control beyond the next statement	0	0	0
v.2: 5.4.2.d	v.2: 5.4.2.d	<b>Unbound arrays</b>	Provides controls to prevent writing beyond the array, string, or buffer boundaries	1	0	0
v.2: 5.4.2.e	v.2: 5.4.2.e	<b>Pointers</b>	Provides controls that prevent pointers from being used to overwrite executable instructions or to access areas where vote counts or audit records are stored	2	0	0
v.2: 5.4.2.f	v.2: 5.4.2.f	<b>Case statements</b>	Default choice explicitly defined	0	0	0
v.2: 5.4.2.g	v.2: 5.4.2.g	<b>Vote counter overflowing</b>	Provides controls to prevent any vote counter from overflowing	0	0	0
v.2: 5.4.2.h	v.2: 5.4.2.h	<b>Indentation</b>	Code is indented consistently and clearly	0	0	0
v.2: 5.4.2.j	v.2: 5.4.2.j	<b>Code generator</b>	Generated code should be marked as such with comments defining the logic invoked	0	0	0
v.2: 5.4.2.k	v.2: 5.4.2.k	<b>Line length</b>	No line of code exceeding 80 columns in width without justification	1	0	0
v.2: 5.4.2.l	v.2: 5.4.2.l	<b>Executable statement</b>	One executable statement for each line of source code	0	0	0
v.2: 5.4.2.m	v.2: 5.4.2.m	<b>Embedded executable statement</b>	The single embedded statement may be considered a part of the conditional expression. Any additional executable statements should be split out to the other lines.	0	0	0
v.2: 5.4.2.n	v.2: 5.4.2.n	<b>Mixed-mode operations</b>	Avoids mixed-mode operations. Comment if mixed-mode usage is necessary.	0	0	0
v.2: 5.4.2.o	v.2: 5.4.2.o	<b>Exit() message</b>	Upon exit() at any point, presents a message to the user indicating the reason for the exit ().	0	0	0
v.2: 5.4.2.p	v.2: 5.4.2.p	<b>Format of messages</b>	Separate and consistent formats to distinguish between normal status and error or exception messages	0	0	0
v.2: 5.4.2.q	v.2: 5.4.2.q	<b>References variables</b>	References variables by fewer than five levels of indirection (i.e. a.b.c.d or a[b].c->d)	0	0	0
v.2: 5.4.2.r	v.2: 5.4.2.r	<b>Levels of indented scope</b>	Functions with fewer than six levels of indented scope	0	0	0
v.2: 5.4.2.s	v.2: 5.4.2.s	<b>Variable initialization</b>	Initializes every variable upon declaration where permitted.	0	0	0
Deleted in VVSG	v.2: 5.4.2.t	<b>Explicit Comparisons</b>	Explicit comparisons in all if() and while() conditions.	0	0	0
v.2: 5.4.2.u	v.2: 5.4.2.u	<b>Constant Definitions</b>	All constants other than "0" and "1" defined or enumerated	2	12	0
v.2: 5.4.2.v	v.2: 5.4.2.v	<b>Ternary Operator</b>	Only contains the minimum implementation of the "a = b ? c : d" syntax. Expansions such as "j=a?(b?c:d):e;" are prohibited.	0	0	0
v.2: 5.4.2.w	v.2: 5.4.2.w	<b>Assert() statement</b>	All assert() statements coded such that they are absent from a production compilation	0	0	0

<b>VVSG</b>	<b>VSS</b>	<b>Requirement</b>	<b>Definition</b>	<b>C &amp; C++</b>	<b>Cobol</b>	<b>VB.Net</b>
	<b>Vol. 1 Section 4.2.7 -Comments</b>					
v.1: 5.2.7.b	v.1: 4.2.7.b	<b>Variables</b>	All variables shall have comments at the point of declaration	<b>8</b>	0	0
v.1: 5.2.7.c	v.1: 4.2.7.c	<b>In-Line Comments</b>	In-line comments shall be provided to facilitate interpretation of functional operations, tests, and branching	<b>2</b>	1	0
v.1: 5.2.7.d	v.1: 4.2.7.d	<b>Assembly code</b>	Assembly code shall contain descriptive and informative comments	0	0	0
v.1: 5.2.7.e	v.1: 4.2.7.e	<b>Comments in uniform format</b>	All comments formatted in a uniform manner	0	0	0
	<b>Vol. 1 Section 6.4.2 -Protection Against Malicious Software</b>					
v1: 7.4.2	v.1: 6.4.2	<b>Malicious Software</b>	Susceptibility to file or macro viruses, worms, Trojan horses, logic bombs, or hardcoded passwords	0	0	0

## **7.3 Appendix C: PCA TDP Documentation Review**

The Unity 3.2.10 PCA TDP Documentation Review listed below reflect the documents submitted for an initial review of the M100 and Document Differences in Unity 3.2.1.0 (see [Section 1 Introduction](#) for the list of document differences.) The tables below reflect the final review results recorded on PCA TDP Document Review. ES&S submitted a complete set of TDP documents that were substantially unchanged from the EAC certified **ESSUnity3200** voting system. The comparison confirming the change was limited to rebranding the document from **ESSUNITY3200** to Unity 3.2.1.0 was noted below. The PCA TDP Document Review for these documents is listed in the **ESSUnity3200** Certification Test Report.

### **7.3.1 Technical Data Package Configuration & Quality Assurance Practices**

Information listed below identifies the results of the review of the TDP Configuration and Quality Assurance practices to the requirements of the VSS 2002/VVSG 2005. During the certification testing iBeta tracked all materials provided by Election Systems and Software. Any time the delivered materials did not conform to the ES&S identified Configuration and Quality Assurance practices were noted in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#) as Informational issues.

### **7.3.2 PCA TDP Document Review**

Information listed summarizes the TDP documents reviewed and the results of their review to the VSS 2002/VVSG 2005 Vol. 2 Sect. 2 requirement.

PCA Document Review Summary	
<b>Vendor</b>	Election Systems & Software
<b>Voting System</b>	Unity v. 3.2.1.0
<b>Scope of Review</b>	Initial review of the M100 TDP and changes to the previously EAC certified <b>ESSUnity3200</b> voting system

<b>VSS Category</b>	<b>Document Name &amp; Version #</b>	<b>Review Date</b>
2.2	Election Systems & Software Voting System Overview Unity v.3.2.1.0 Ver. 6.0	1/21/2010
2.2	Election Systems & Software System Limitations Unity v.3.2.1.0 Ver. 6.0	1/21/2010
2.2:	Reuse Unity 3200 Section 2.2 changes have no impact	1/20/2010
2.3:	ES&S System Functionality Description Hardware Programming Manager (HPM) Unity v.3.2.1.0 Ver. 3.0	1/22/2010
2.3:	Reuse Unity 3200 Section 2.3 changes have no impact	1/20/2010
2.3:	ES&S System Functionality Description Model 100 Unity v. 3.2.1.0 ver. 10.0	1/22/2010
2.3:	Election Systems & Software ES&S System Functionality Description Ver. 3.0	8/16/2009
2.4:	ES&S System Hardware Specification Model 100 Unity v. 3.2.1.0 - v.3.0	8/17/2009
2.4:	INDENTED BILL OF MATERIAL (Model 100) - No version	8/17/2009
2.4:	Reuse Unity 3200 Section 2.4 changes have no impact	1/21/2010
2.5:	ES&S Software Design Specifications Model 100, v.3.0	8/14/2009
2.5:	Reuse Unity 3200 Section 2.5 changes have no impact	5/3/2010
2.6:	Reuse Unity 3200 Section 2.6 changes have no impact	2/15/2010
2.6:	ES&S System Security Specification Version Release 3.2.1.0 February 12, 2010	2/15/2010
2.6	Hardening Procedures for the Election Management System PC August 11th 2009	8/19/2009

VSS Category	Document Name & Version #	Review Date
2.6	Engineering Programmer Quick Start Guide No version	8/19/2009
2.6	Election Systems & Software Model 100 Validation Guide August 11th 2009	8/19/2009
2.7	Reuse of Unity 3.2 System Test and Verification Specification	8/24/2009
2.7	Model 100 Test Case Specification Firmware Version 5.4.0.0 Hardware Version 1.3 Test Case 1.0	1/22/2010
2.7	DS200 Test Cases Unity 3.2.1.0 Version 1.3.11.0	1/22/2010
2.7	Audit Manager Test Case Specifications Software Version 7.5.2.0 Test Case 1.0	1/23/2010
2.8	ES&S Model 100 System Operations Procedures Firmware Version 5.4.0.0 Hardware revision 1.3	8/17/2009
2.8	Reuse Unity 3200 Section 2.8 changes have no impact	1/21/2010
2.8	ES&S Election Reporting Manager System Operations Procedures Version Release 7.5.5.0 1/8/10	1/21/2010
2.8	ES&S Image Manager System Operations Procedures Version Release 7.7.1.0 1/8/10	1/21/2010
2.8	ES&S Ballot On Demand Printer Setup and Printing Procedures Version Release 7.7.1.0 Okidata part number 58273508 1/8/10	1/21/2010
2.8	ES&S Hardware Programming Manager System Operations Procedures Version Release 5.7.1.0 1/8/10	1/21/2010
2.8	Setting the Date and Time on a Model 650 Scanner 5/13/08	1/21/2010
2.8	ES&S LogMonitor System Operations Procedures LogMonitor 1.0.0.0 8/28/09	1/21/2010
2.8	Election Data Manager (EDM) Checklist Election Day Training Manual Unity Version 3.2.1.0 No Version	1/21/2010
2.8	AutoMARK Information Management System Election Official's Guide Rev 18	1/26/2010
2.9	ES&S M100 System Maintenance Manual Firmware Version 5.4.0.0 Hardware Version 1.3 8/11/09	1/25/2010
2.9	ES&S Ballot Production Handbook Version 1.0.0.0 July 17, 2007	8/17/2009
2.9	Reuse Unity 3200 Section 2.8 changes have no impact	1/21/2010
2.9:	DS200 System Maintenance Manual Hardware Version 1.2.1.0 Firmware Version 1.3.11.0 10/21/09	1/26/2010
2.10	Reuse of Unity 3.2 Personnel Deployment and Training Recommendations	8/17/2009
2.10	Training Checklist M100: Pre-Election 7/31/09	8/17/2009
2.10	Training Checklist M100: Election Day 7/31/09	8/17/2009
2.10	Reuse Unity 3200 Section 2.10 changes have no impact	1/21/2010
2.10	Model 650 Pre-Election Day Checklist Version Number 2.2.x	1/25/2010
2.10	Election Data Manager Training Manual Version Number 7.8.x 7/31/09	1/25/2010
2.10	Election Reporting Manager Pre-Election Day Training Manual Version Number 7.5.x 7/31/09	1/25/2010
2.10	ESSIM Training Manual Version Number 7.7.x 7/31/09	1/25/2010
2.10	Hardware Program Manager Training Manual Version Number 5.7.x 7/31/09	1/26/2010
2.10	Election Results Export (EXP) Election Day Checklist Version Number 3.0.x 7/31/09	1/26/2010
2.10	Audit Manager Training Manual Version 7.5.x 7/31/09	1/26/2010
2.10	AutoMARK Election Day Checklist Version Number 1.3.x 7/31/09	1/26/2010
2.10	AutoMARK Pre-Election Day Checklist Version Number 1.3.x 7/31/09	1/26/2010
2.11	ES&S Configuration Management Plan Version 2.0	1/25/2010
2.11	Reuse Unity 3200 Section 2.11 changes have no impact	1/20/2010
2.11	AutoMARK Voter Assist Terminal (VAT) - Version 1.3 & 1.4 Firmware, Hardware & Windows CE Operating System Installation Instructions ver. 15	1/26/2010
2.11	AutoMARK AIMS Software Compilation Instructions Rev 2	1/27/2010

VSS Category	Document Name & Version #	Review Date
2.12	Reuse Unity 3200 Section 2.12 changes have no impact	1/20/2010
2.13	Unity 3.2.1.0 System Change Notes Rev 3.0	1/25/2010
2.13	AIMS System Change Notes Rev 26	1/26/2010

**Review Criteria:**

\*\*\* The specific requirement is not applicable to the category of documents reviewed

**Accept** Meets the requirement

**Reject** Does not meet the requirement

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
2.1	<b>Scope</b>												
2.1.1.2	<b>Required Content for System Changes and Re-qualification</b>												
	If the scope of this certification is a change verify that the vendor has submitted appropriate System Change Notes covering this document. If this is not a change, no change notes are required.	Accept											
2.1.1.3	<b>Format</b>												
	The TDP shall include a detailed table of contents for the required documents.	Accept											
2.1.3	<b>Protection of Proprietary Information</b>												
	Verify that if the vendor considers this document proprietary, they have marked it as such. Documents that are approved by the vendor for public release do not need to be marked.	Accept											
2.2	<b>System Overview</b>												
	In the system overview, the vendor shall provide information that enables the accredited test lab to identify the functional and physical components of the system, how the components are structured, and the interfaces between them.	Accept	***	***	***	***	***	***	***	***	***	***	***
2.2.1	<b>System Description -</b> The system description shall include written descriptions, drawings and diagrams that present:												
a.	A description of the functional components (or subsystems) as defined by the vendor (e.g., environment, election management and control, vote recording, vote conversion, reporting, and their interconnection)	Accept	***	***	***	***	***	***	***	***	***	***	***
b.	A description of the operational environment of the system that provides an overview of the hardware, software, and communications structure	Accept	***	***	***	***	***	***	***	***	***	***	***
c.	A concept of operations that explains each system function, and how the function is achieved in the design	Accept	***	***	***	***	***	***	***	***	***	***	***
d.	Descriptions of the functional and physical interfaces between subsystems and components	Accept	***	***	***	***	***	***	***	***	***	***	***
e.	Identification of all COTS hardware and software products and communications services used in the development and/or operation of the voting system, identifying the name, vendor, and version used for each such component, including:	Accept	***	***	***	***	***	***	***	***	***	***	***

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
1)	Operating Systems	Accept	***	***	***	***	***	***	***	***	***	***	***
2)	Database software	Accept	***	***	***	***	***	***	***	***	***	***	***
3)	Communications routers	Accept	***	***	***	***	***	***	***	***	***	***	***
4)	Modem drivers	Accept	***	***	***	***	***	***	***	***	***	***	***
5)	Dial-up networking software	Accept	***	***	***	***	***	***	***	***	***	***	***
f.	Interfaces among internal components, and interfaces with external systems. For components that interface with other components for which multiple products may be used, the TDP shall provide an identification of:	Accept	***	***	***	***	***	***	***	***	***	***	***
1)	File specifications, data objects, or other means used for information exchange	Accept	***	***	***	***	***	***	***	***	***	***	***
2)	The public standard used for such file specifications, data objects, or other means	Accept	***	***	***	***	***	***	***	***	***	***	***
g.	Benchmark directory listings for all software (including firmware elements) and associated documentation included in the vendor's release in order of how each piece of software would normally be installed upon setup and installation.	Accept	***	***	***	***	***	***	***	***	***	***	***
<b>2.2.2</b>	<b>System Performance -</b> The vendor shall provide system performance information including:												
a.	The performance characteristics of each operating mode and function in terms of expected and maximum speed, throughput capacity, maximum volume (maximum number of voting positions and maximum number of ballot styles supported), and processing frequency	Accept	***	***	***	***	***	***	***	***	***	***	***
b.	Quality attributes such as reliability, maintainability, availability, usability, and portability	Accept	***	***	***	***	***	***	***	***	***	***	***
c.	Provisions for safety, security, privacy, and continuity of operation	Accept	***	***	***	***	***	***	***	***	***	***	***
d.	Design constraints, applicable standards, and compatibility requirements	Accept	***	***	***	***	***	***	***	***	***	***	***
<b>2.3</b>	<b>System Functionality Description</b>												
	The vendor shall declare the scope of the system's functional capabilities, thereby establishing the performance, design, test, manufacture, and acceptance context for the system.	***	Accept	***	***	***	***	***	***	***	***	***	***
	The vendor shall provide a listing of the system's functional processing capabilities, encompassing capabilities required by the Guidelines and any additional capabilities provided by the system. This listing shall provide a simple description of each capability. Detailed specifications shall be provided in other documentation required for the TDP.	***	Accept	***	***	***	***	***	***	***	***	***	***
a.	The vendor shall organize the presentation of required capabilities in a manner that corresponds to the structure and sequence of functional capabilities indicated in Volume I, Section 2. The contents of Volume I, Section 2 may be used as the basis for a checklist to indicate the	***	Accept	***	***	***	***	***	***	***	***	***	***

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
	specific functions provided and those not provided by the system.												
b.	Additional capabilities shall be clearly indicated.	***	Accept	***	***	***	***	***	***	***	***	***	***
c.	Required capabilities that may be bypassed or deactivated during installation or operation by the user shall be clearly indicated	***	Accept	***	***	***	***	***	***	***	***	***	***
d.	Additional capabilities that function only when activated during installation or operation by the user shall be clearly indicated	***	Accept	***	***	***	***	***	***	***	***	***	***
e.	Additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user shall be clearly indicated.	***	Accept	***	***	***	***	***	***	***	***	***	***
<b>2.4</b>	<b>System Hardware Specifications</b>												
	The vendor shall expand on the system overview by providing detailed specifications of the hardware components of the system, including specifications of hardware used to support the telecommunications capabilities of the system, if applicable.	***	***	Accept	***	***	***	***	***	***	***	***	***
<b>2.4.1</b>	<b>System Hardware Characteristics</b>												
	The vendor shall provide a detailed discussion of the characteristics of the system, indicating how the hardware meets individual requirements defined in Volume I, Sections 3, 4, 5, and 6 of the standards and include:	***	***	Accept	***	***	***	***	***	***	***	***	***
a.	<b>Performance Characteristics:</b> This discussion addresses basic system performance attributes and operational scenarios that describe the manner in which system functions are invoked, describes environmental capabilities, describes life expectancy, and describes any other essential aspects of system performance	***	***	Accept	***	***	***	***	***	***	***	***	***
b.	<b>Physical Characteristics:</b> This discussion addresses suitability for intended use, requirements for transportation and storage, health and safety criteria, security criteria, and vulnerability to adverse environmental factors	***	***	Accept	***	***	***	***	***	***	***	***	***
c.	<b>Reliability:</b> This discussion addresses system and component reliability stated in terms of the systems operating functions, and identification of items that require special handling or operation to sustain system reliability	***	***	Accept	***	***	***	***	***	***	***	***	***
d.	<b>Maintainability:</b> The discussion addresses maintainability. Maintainability represents the ease with which maintenance actions can be performed based on the design characteristics of equipment and software and the processes the vendor and election officials have in place for preventing failures and for reacting to failures. Maintainability includes the ability of equipment and software to self-diagnose problems and to make non-technical election workers aware of a problem. Maintainability also addresses a range of scheduled and unscheduled events	***	***	Accept	***	***	***	***	***	***	***	***	***
e.	<b>Environmental Conditions:</b> This discussion addresses the ability of the system to withstand natural environments, and operational constraints in normal and test environments, including all requirements and restrictions regarding electrical service, telecommunications services, environmental protection, and any additional facilities or resources required to install and operate the	***	***	Accept	***	***	***	***	***	***	***	***	***

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
	system												
<b>2.4.2</b>	<b>Design and Construction</b>												
	The vendor shall provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for testing.	***	***	Accept	***	***	***	***	***	***	***	***	***
	The vendor shall provided a list of materials and components used in the system, a description of their assembly into major system components and the system as a whole. Paragraphs and diagrams shall be provided that describe:	***	***	Accept	***	***	***	***	***	***	***	***	***
a.	Materials, processes, and parts used in the system, their assembly, and the configuration control measures to ensure compliance with the system specification	***	***	Accept	***	***	***	***	***	***	***	***	***
b.	The electromagnetic environment generated by the system	***	***	Accept	***	***	***	***	***	***	***	***	***
c.	Operator and voter safety considerations, and any constraints on system operations or the use environment	***	***	Accept	***	***	***	***	***	***	***	***	***
d.	Human engineering considerations, including provisions for access by disabled voters	***	***	Accept	***	***	***	***	***	***	***	***	***
<b>2.5</b>	<b>Software Design and Specification</b>												
	The vendor shall expand on the system overview by providing detailed specifications of the software components of the system, including software used to support the telecommunications capabilities of the system, if applicable.	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.1</b>	<b>Purpose and Scope</b>												
	The vendor shall describe the function or functions that are performed by the software programs that comprise the system, including software used to support the telecommunications capabilities of the system, if applicable.	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.2</b>	<b>Applicable Documents</b>												
	The vendor has listed all documents controlling the development of the software and its specifications. Documents shall be listed in order of precedence.	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.3</b>	<b>Software Overview</b> The vendor shall provide an overview of the software that includes the following items:												
a.	A description of the software system concept, including specific software design objectives, and the logic structure and algorithms used to accomplish these objectives	***	***	***	Accept	***	***	***	***	***	***	***	***
b.	The general design, operational considerations, and constraints influencing the design of the software	***	***	***	Accept	***	***	***	***	***	***	***	***
c. 1) 2) 3)	Identification of all software items, indicating items that were: - Written in-house - Procured and not modified - Procured and modified, including descriptions of the modifications to the software and to the default configuration options	***	***	***	Accept	***	***	***	***	***	***	***	***
d. 1) 2)	Additional information for each item that includes: - Item identification - General description	***	***	***	Accept	***	***	***	***	***	***	***	***

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
3)	- Software requirements performed by the item												
4)	- Identification of interfaces with other items that provide data to, or receive data from, the item												
5)	- Concept of execution for the item												
	The vendor shall also include a certification that procured software items were obtained directly from the manufacturer or a licensed dealer or distributor.	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.4</b>	<b>Software Standards and Conventions</b>												
	The vendor shall provide information that can be used by an accredited test lab or state certification board to support software analysis and test design. The information addresses standards and conventions developed internally by the vendor as well as published industry standards applied by the vendor. The vendor shall provide information addressing standards and conventions for:	***	***	***	Accept	***	***	***	***	***	***	***	***
a.	Software system development methodology	***	***	***	Accept	***	***	***	***	***	***	***	***
b.	Software design standards, including internal vendor procedures	***	***	***	Accept	***	***	***	***	***	***	***	***
c.	Software specification standards, including internal vendor procedures	***	***	***	Accept	***	***	***	***	***	***	***	***
d.	Software coding standards, including internal vendor procedures	***	***	***	Accept	***	***	***	***	***	***	***	***
e.	Testing and verification standards, including internal vendor procedures, that can assist in determining the program's correctness and ACCEPT/REJECT criteria	***	***	***	Accept	***	***	***	***	***	***	***	***
f.	Quality assurance standards or other documents that can be used to examine and test the software. These documents include standards for program flow and control charts, program documentation, test planning, and for test data acquisition and reporting	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.5</b>	<b>Software Operating Environment</b>												
	This section shall describe or makes reference to all operating environment factors that influence the software design.	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.5.1</b>	<b>Hardware Environment and Constraints</b>												
	The vendor shall identify and describe the hardware characteristics that influence the design of the software, such as												
a.	The logic and arithmetic capability of the processor	***	***	***	Accept	***	***	***	***	***	***	***	***
b.	Memory read-write characteristics	***	***	***	Accept	***	***	***	***	***	***	***	***
c.	External memory device characteristics	***	***	***	Accept	***	***	***	***	***	***	***	***
d.	Peripheral device interface hardware	***	***	***	Accept	***	***	***	***	***	***	***	***
e.	Data input/output device protocols	***	***	***	Accept	***	***	***	***	***	***	***	***
f.	Operator controls, indicators, and displays	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.5.2</b>	<b>Software Environment</b>												
	The vendor shall identify the compilers or assemblers used in the generation of executable code, and described the operating system or system monitor.	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.6</b>	<b>Software Functional Specification</b>												
	The vendor shall provide a description of the operating modes of the system and of software capabilities to perform specific functions.	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.6.1</b>	<b>Configurations and Operating Modes</b>												
	The vendor shall describe all software configurations and operating modes of the system, such as ballot preparation, election	***	***	***	Accept	***	***	***	***	***	***	***	***

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
	programming, preparation for opening the polling place, recording votes and/or counting ballots, closing the polling place, and generating reports. For each software function or operating mode, the vendor shall provide:												
a.	A definition of the inputs to the function or mode (with characteristics, tolerances or acceptable ranges, as applicable)	***	***	***	Accept	***	***	***	***	***	***	***	***
b.	An explanation of how the inputs are processed	***	***	***	Accept	***	***	***	***	***	***	***	***
c.	A definition of the outputs produced (again, with characteristics, tolerances, or acceptable ranges as applicable).	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.6.2</b>	<b>Software Functions</b> <b>The vendor shall describe the software's capabilities or methods for detecting or handling</b>												
a.	Exception conditions	***	***	***	Accept	***	***	***	***	***	***	***	***
b.	System failures	***	***	***	Accept	***	***	***	***	***	***	***	***
c.	Data input/output errors	***	***	***	Accept	***	***	***	***	***	***	***	***
d.	Error logging for audit record generation	***	***	***	Accept	***	***	***	***	***	***	***	***
e.	Production of statistical ballot data	***	***	***	Accept	***	***	***	***	***	***	***	***
f.	Data quality assessment	***	***	***	Accept	***	***	***	***	***	***	***	***
g.	Security monitoring and control.	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.7</b>	<b>Programming Specifications</b>												
	The vendor shall provide in this section an overview of the software design, its structure, and implementation algorithms and detailed specifications for individual software modules.	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.7.1</b>	<b>Programming Specifications Overview</b>												
	The overview shall include such items as flowcharts, HIPOs, data flow diagrams, and other graphical techniques that facilitate understanding of the programming specifications. This section shall be prepared to facilitate understanding of the internal functioning of the individual software modules. Implementation of the functions shall be described in terms of the software architecture, algorithms, and data structures.	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.7.2</b>	<b>Programming Specifications Details</b> The programming specifications shall describe individual software modules and their component units, if applicable and for each module and unit, the vendor shall provide:												
a.	Module and unit design decisions, if any, such as algorithms used	***	***	***	Accept	***	***	***	***	***	***	***	***
b.	Any constraints, limitations, or unusual features in the design of the software module or unit	***	***	***	Accept	***	***	***	***	***	***	***	***
c.	The programming language to be used and rationale for its use if other than the specified module or unit language	***	***	***	Accept	***	***	***	***	***	***	***	***
d.	If the software module or unit consists of or contains procedural commands, (such as menu selections in a database management system (DBMS) for defining forms and reports, on-line DBMS queries for database access and manipulation, input to a graphical user interface (GUI) builder for automated code generation, commands to the operating system, or shell scripts) a list of the procedural commands and reference to user manuals or other documents that explain them	***	***	***	Accept	***	***	***	***	***	***	***	***

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
e.	If the software module or unit contains, receives, or outputs data, a description of its inputs, outputs, and other data elements as applicable. (Section 2.5.9 describes the requirements for documenting system interfaces.) Data local to the software module or unit shall be described separately from data input to or output from the software module or unit)	***	***	***	Accept	***	***	***	***	***	***	***	***
f.	If the software module or unit contains logic, verify the logic to be used by the software unit, including, as applicable:	***	***	***	Accept	***	***	***	***	***	***	***	***
f.1	Conditions in effect within the software module or unit when its execution is initiated	***	***	***	Accept	***	***	***	***	***	***	***	***
f.2	Conditions under which control is passed to other software modules or units	***	***	***	Accept	***	***	***	***	***	***	***	***
f.3	Response and response time to each input, including data conversion, renaming, and data transfer operation	***	***	***	Accept	***	***	***	***	***	***	***	***
f.4	Sequence of operations and dynamically controlled sequencing during the software module's or unit's operation, including:	***	***	***	Accept	***	***	***	***	***	***	***	***
f.4.i	The method for sequence control	***	***	***	Accept	***	***	***	***	***	***	***	***
f.4.ii	The logic and input conditions of that method, such as timing variations, priority assignments	***	***	***	Accept	***	***	***	***	***	***	***	***
f.4.iii	Data transfer in and out of memory	***	***	***	Accept	***	***	***	***	***	***	***	***
f.4.iv	The sensing of discrete input signals, and timing relationships between interrupt operations within the software module or unit	***	***	***	Accept	***	***	***	***	***	***	***	***
f.5	Exception and error handling	***	***	***	Accept	***	***	***	***	***	***	***	***
g.	If the software module is a database, the vendor provides the information described in subsection 2.5.8.	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.8 System Database</b>													
	The vendor shall identify and provide a diagram and narrative description of the system's databases, and any external files used for data input or output. The information provided shall include for each database or external file:	***	***	***	Accept	***	***	***	***	***	***	***	***
a	The number of levels of design and the names of those levels (such as conceptual, internal, logical, and physical)	***	***	***	Accept	***	***	***	***	***	***	***	***
b.	Design conventions and standards (which may be incorporated by references) needed to understand the design	***	***	***	Accept	***	***	***	***	***	***	***	***
c.	Identification and description of all database entities and how they are implemented physically (e.g., tables, files)	***	***	***	Accept	***	***	***	***	***	***	***	***
d.	Entity relationship diagram and description of relationships	***	***	***	Accept	***	***	***	***	***	***	***	***
e.	Details of table, record or file contents (as applicable) to include individual data elements and their specifications, including:	***	***	***	Accept	***	***	***	***	***	***	***	***
1)	Names/identifiers	***	***	***	Accept	***	***	***	***	***	***	***	***
2)	Data type (alphanumeric, integer, etc.)	***	***	***	Accept	***	***	***	***	***	***	***	***
3)	Size and format (such as length and punctuation of a character string)	***	***	***	Accept	***	***	***	***	***	***	***	***
4)	Units of measurement (such as meters, dollars, nanoseconds)	***	***	***	Accept	***	***	***	***	***	***	***	***
5)	Range or enumeration of possible values (such as 0-99)	***	***	***	Accept	***	***	***	***	***	***	***	***
6)	Accuracy (how correct) and precision (number of significant digits)	***	***	***	Accept	***	***	***	***	***	***	***	***
7)	Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether	***	***	***	Accept	***	***	***	***	***	***	***	***

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
	business rules apply												
8)	Security and privacy constraints	***	***	***	Accept	***	***	***	***	***	***	***	***
9)	Sources (setting/sending entities) and recipients (using/receiving entities).	***	***	***	Accept	***	***	***	***	***	***	***	***
f.	For external files, a description of the procedures for file maintenance, management of access privileges, and security.	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.9</b>	<b>Interfaces</b>												
	The vendor shall identify and provides a complete description of all internal and external interfaces, using a combination of text and diagrams	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.9.1</b>	<b>Interface Identification</b> For each interface identified in the system overview, the vendor shall:												
a.	Provide a unique identifier assigned to the interface	***	***	***	Accept	***	***	***	***	***	***	***	***
b.	Identify the interfacing entities (systems, configuration items, users, etc.) by name, number, version, and documentation references, as applicable	***	***	***	Accept	***	***	***	***	***	***	***	***
c.	Identify which entities have fixed interface characteristics (and therefore impose interface requirements on interfacing entities) and which are being developed or modified (thus having interface requirements imposed on them).	***	***	***	Accept	***	***	***	***	***	***	***	***
<b>2.5.9.2</b>	<b>Interface Description</b> For each interface identified in the system overview, the vendor shall provide information that describes:												
a.	The type of interface (such as real-time data transfer, storage-and-retrieval of data, etc.) to be implemented	***	***	***	Accept	***	***	***	***	***	***	***	***
b.	Characteristics of individual data elements that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:	***	***	***	Accept	***	***	***	***	***	***	***	***
1)	Names/identifiers	***	***	***	Accept	***	***	***	***	***	***	***	***
2)	Data type (alphanumeric, integer, etc.)	***	***	***	Accept	***	***	***	***	***	***	***	***
3)	Size and format (such as length and punctuation of a character string)	***	***	***	Accept	***	***	***	***	***	***	***	***
4)	Units of measurement (such as meters, dollars, nanoseconds)	***	***	***	Accept	***	***	***	***	***	***	***	***
5)	Range or enumeration of possible values (such as 0-99)	***	***	***	Accept	***	***	***	***	***	***	***	***
6)	Accuracy (how correct) and precision (number of significant digits)	***	***	***	Accept	***	***	***	***	***	***	***	***
7)	Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply	***	***	***	Accept	***	***	***	***	***	***	***	***
8)	Security and privacy constraints and	***	***	***	Accept	***	***	***	***	***	***	***	***
9)	Sources (setting/sending entities) and recipients (using/receiving entities)	***	***	***	Accept	***	***	***	***	***	***	***	***
c.	Characteristics of communication methods that the interfacing entity(ies) will use for the interface, such as:	***	***	***	Accept	***	***	***	***	***	***	***	***
1)	Communication links/bands/frequencies/media and their characteristics	***	***	***	Accept	***	***	***	***	***	***	***	***
2)	Message formatting	***	***	***	Accept	***	***	***	***	***	***	***	***
3)	Flow control (such as sequence numbering and buffer allocation)	***	***	***	Accept	***	***	***	***	***	***	***	***
4)	Data transfer rate, whether periodic/aperiodic, and interval between transfers	***	***	***	Accept	***	***	***	***	***	***	***	***

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
5)	Routing, addressing, and naming conventions	***	***	***	Accept	***	***	***	***	***	***	***	***
6)	Transmission services, including priority and grade and	***	***	***	Accept	***	***	***	***	***	***	***	***
7)	Safety/security/privacy considerations, such as encryption, user authentication, compartmentalization, and auditing	***	***	***	Accept	***	***	***	***	***	***	***	***
d.	Characteristics of protocols the interfacing entity(ies) will use for the interface, such as:	***	***	***	Accept	***	***	***	***	***	***	***	***
1)	Priority/layer of the protocol	***	***	***	Accept	***	***	***	***	***	***	***	***
2)	Packeting, including fragmentation and reassembly, routing, and addressing	***	***	***	Accept	***	***	***	***	***	***	***	***
3)	Legality checks, error control, and recovery procedures	***	***	***	Accept	***	***	***	***	***	***	***	***
4)	Synchronization, including connection establishment, maintenance, termination	***	***	***	Accept	***	***	***	***	***	***	***	***
5)	Status, identification, and any other reporting features	***	***	***	Accept	***	***	***	***	***	***	***	***
e.	Other characteristics, such as physical compatibility of the interfacing entity(ies) (dimensions, tolerances, loads, voltages, plug compatibility, etc.).	***	***	***	Accept	***	***	***	***	***	***	***	***
2.5.10	<b>Appendices</b> The vendor may provide descriptive material and data supplementing the various sections of the body of the Software Specifications. The content and arrangement of appendices shall be at the discretion of the vendor. Topics recommended for amplification or treatment in appendix form include:  Glossary: A listing and brief definition of all software module names and variable names, with reference to their locations in the software structure. Abbreviations, acronyms, and terms should be included, if they are either uncommon in data processing and software development or are used in an unorthodox semantic References: A list of references to all related vendor documents, data, standards, and technical sources used in software development and testing Program Analysis: The results of software configuration analysis algorithm analysis and selection, timing studies, and hardware interface studies that are reflected in the final software design and coding												
2.6	<b>System Security Specification</b>												
	The vendor shall submit a system security specification that addresses the security requirements of Volume I, Section 6, and describes the level of security provided by the system in terms of the specific security risks addressed by the system, the means by which each risk is addressed, the process used to test and verify the effective operation of security capabilities and, for systems that use public telecommunications networks as defined in Volume I, Section 5, the means used to keep the security capabilities of the system current to respond to the evolving threats against these systems.	***	***	***	***	Accept	***	***	***	***	***	***	***
2.6.1	<b>Access Control Policy</b>												
	The vendor shall specify the features and capabilities of the access control policy recommended to purchasing jurisdictions to provide	***	***	***	***	Accept	***	***	***	***	***	***	***

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
	effective voting system security to meet the specific requirements of Volume I, Section 6.2.1. The access control policy shall address the general features and capabilities and individual access privileges indicated in Volume I, Section 6.2.1.												
<b>2.6.2</b>	<b>Access Control Measures</b>												
	The vendor shall provide a detailed description of all system access control measures and mandatory procedures designed to permit access to system states in accordance with the access policy, and to prevent all other types of access to meet the specific requirements of Volume I, Section 6.2.2.	***	***	***	***	Accept	***	***	***	***	***	***	***
	The vendor shall also define and provide a detailed description of the methods used to preclude unauthorized access to the access control capabilities of the system itself.	***	***	***	***	Accept	***	***	***	***	***	***	***
<b>2.6.3</b>	<b>Equipment and Data Security</b>												
	The vendor shall provide a detailed description of system capabilities and mandatory procedures for purchasing jurisdictions to prevent disruption of the voting process and corruption of voting data to meet the specific requirements of Volume I, Section 6.3 of the Standards. This information shall address measures for polling place security and central count location security.	***	***	***	***	Accept	***	***	***	***	***	***	***
<b>2.6.4</b>	<b>Software Installation</b>												
	The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure software (including firmware) installation to meet the specific requirements of Volume I, Section 6.4 of the Standards. This information shall address software installation for all system components.	***	***	***	***	Accept	***	***	***	***	***	***	***
<b>2.6.5</b>	<b>Telecommunications and Data Transmission Security</b>												
	The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure data transmission to meet the specific requirements of Volume I, Section 6.5:	***	***	***	***	Accept	***	***	***	***	***	***	***
a.	For all systems, this information shall address access control, and prevention of data interception	***	***	***	***	Accept	***	***	***	***	***	***	***
b.	For systems that use public communications networks as defined in Volume I, Section 5, this information shall also include:	***	***	***	***	Accept	***	***	***	***	***	***	***
1)	Capabilities used to provide protection against threats to third party products and services	***	***	***	***	Accept	***	***	***	***	***	***	***
2)	Policies and processes used by the vendor to ensure that such protection is updated to remain effective over time	***	***	***	***	Accept	***	***	***	***	***	***	***
3)	Policies and procedures used by the vendor to ensure that current versions of such capabilities are distributed to user jurisdictions and are installed effectively by the jurisdiction	***	***	***	***	Accept	***	***	***	***	***	***	***
4)	A detailed description of the system capabilities and procedures to be employed by the jurisdiction to diagnose the occurrence of a denial of service attack, to use an alternate method of voting, to determine when it is appropriate to resume voting over the network, and to	***	***	***	***	Accept	***	***	***	***	***	***	***

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
	consolidate votes cast using the alternate method												
5)	A detailed description of all activities to be performed in setting up the system for operation that are mandatory to ensure effective system security, including testing of security before an election and	***	***	***	***	Accept	***	***	***	***	***	***	***
6)	A detailed description of all activities that should be prohibited during system setup and during the timeframe for voting operations, including both the hours when polls are open and when polls are closed.	***	***	***	***	Accept	***	***	***	***	***	***	***
<b>2.6.6</b>	<b>Other Elements of an Effective Security Program</b>												
	The vendor shall provide a detailed description of additional procedures required for use by the purchasing jurisdiction including:	***	***	***	***	Accept	***	***	***	***	***	***	***
a.	Administrative and management controls for the voting system and election management, including access controls	***	***	***	***	Accept	***	***	***	***	***	***	***
b.	Internal security procedures, including operating procedures for maintaining the security of the software for each system function and operating mode	***	***	***	***	Accept	***	***	***	***	***	***	***
c.	Adherence to, and enforcement of, operational procedures (e.g., effective password management)	***	***	***	***	Accept	***	***	***	***	***	***	***
d.	Physical facilities and arrangements	***	***	***	***	Accept	***	***	***	***	***	***	***
e.	Organizational responsibilities and personnel screening.	***	***	***	***	Accept	***	***	***	***	***	***	***
<b>2.7</b>	<b>System Test and Verification Specification</b>												
	The vendor shall provide test and verification specifications for:												
a.	Development test specifications	***	***	***	***	***	Accept	***	***	***	***	***	***
b.	Qualification test specifications.	***	***	***	***	***	Accept	***	***	***	***	***	***
<b>2.7.1</b>	<b>Development Test Specifications</b>												
	The vendor shall describe the plans, procedures, and data used during software development and system integration to verify system logic correctness, data quality, and security. This description shall include:	***	***	***	***	***	Accept	***	***	***	***	***	***
a.	Test identification and design, including:	***	***	***	***	***	Accept	***	***	***	***	***	***
1)	Test structure	***	***	***	***	***	Accept	***	***	***	***	***	***
2)	Test sequence or progression	***	***	***	***	***	Accept	***	***	***	***	***	***
3)	Test conditions	***	***	***	***	***	Accept	***	***	***	***	***	***
b.	Standard test procedures, including any assumptions or constraints	***	***	***	***	***	Accept	***	***	***	***	***	***
c.	Special purpose test procedures including any assumptions or constraints	***	***	***	***	***	Accept	***	***	***	***	***	***
d.	Test data, test data source, whether it is real or simulated, and control of test data	***	***	***	***	***	Accept	***	***	***	***	***	***
e.	Expected test results	***	***	***	***	***	Accept	***	***	***	***	***	***
f.	Criteria for evaluating test results.	***	***	***	***	***	Accept	***	***	***	***	***	***
<b>2.7.2</b>	<b>Qualification Test Specifications</b>												
	The vendor shall provide specifications for verification and validation of overall software performance. The specifications shall cover:	***	***	***	***	***	Accept	***	***	***	***	***	***
a.	Control and data input/output	***	***	***	***	***	Accept	***	***	***	***	***	***
b.	Acceptance criteria	***	***	***	***	***	Accept	***	***	***	***	***	***
c.	Processing accuracy	***	***	***	***	***	Accept	***	***	***	***	***	***
d.	Data quality assessment and maintenance	***	***	***	***	***	Accept	***	***	***	***	***	***

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
e.	Ballot interpretation logic	***	***	***	***	***	Accept	***	***	***	***	***	***
f.	Exception handling	***	***	***	***	***	Accept	***	***	***	***	***	***
g.	Security	***	***	***	***	***	Accept	***	***	***	***	***	***
h.	Production of audit trails and statistical data.	***	***	***	***	***	Accept	***	***	***	***	***	***
	The specifications shall identify procedures for assessing and demonstrating the suitability of the software for elections use.	***	***	***	***	***	Accept	***	***	***	***	***	***
<b>2.8</b>	<b>System Operations Procedures</b>												
	This documentation shall provide all information necessary for system use by all personnel who support pre-election and election preparation, polling place activities and central counting activities, as applicable, with regard to all system functions and operations identified in Section 2.3 above. The nature of instructions for operating personnel will depend upon the overall system design and required skill level of system operations support personnel.	***	***	***	***	***	***	Accept	***	***	***	***	***
	The system operations procedures shall contain all information that is required for the preparation of detailed system operating procedures, and for operator training, as described below:	***	***	***	***	***	***	Accept	***	***	***	***	***
<b>2.8.1</b>	<b>Introduction</b>												
	The vendor shall provide a summary of system operating functions and modes, in sufficient detail to permit understanding of the system's capabilities and constraints. The roles of operating personnel shall be identified and related to the operating modes of the system. Decision criteria and conditional operator functions (such as error and failure recovery actions) shall be described.	***	***	***	***	***	***	Accept	***	***	***	***	***
	The vendor shall also list all reference and supporting documents pertaining to the use of the system during elections operations.	***	***	***	***	***	***	Accept	***	***	***	***	***
<b>2.8.2</b>	<b>Operational Environment</b>												
	The vendor shall describe the system environment, and the interface between the user or operator and the system.	***	***	***	***	***	***	Accept	***	***	***	***	***
a.	The vendor shall identify all facilities, furnishings, fixtures, and utilities that will be required, including equipment that operates at the: Polling place	***	***	***	***	***	***	Accept	***	***	***	***	***
b.	Central count facility	***	***	***	***	***	***	Accept	***	***	***	***	***
c.	Other locations	***	***	***	***	***	***	Accept	***	***	***	***	***
<b>2.8.3</b>	<b>System Installation and Test Specification</b>												
	The vendor shall provide specifications for validation of system installation, acceptance, and readiness. These specifications address all components of the system, all locations of installation (e.g., polling place central count facility), and all elements of system functionality and operations identified in Section 2.3 above, including:	***	***	***	***	***	***	Accept	***	***	***	***	***
a.	Pre-voting functions	***	***	***	***	***	***	Accept	***	***	***	***	***
b.	Voting functions	***	***	***	***	***	***	Accept	***	***	***	***	***
c.	Post-voting functions	***	***	***	***	***	***	Accept	***	***	***	***	***
d.	General capabilities	***	***	***	***	***	***	Accept	***	***	***	***	***
<b>2.8.4</b>	<b>Operational Features</b>												
	The vendor shall provide the documentation of system operating features that meets the following requirements:												

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
a.	A detailed description of all input, output, control, and display features accessible to the operator or voter	***	***	***	***	***	***	Accept	***	***	***	***	***
b.	Examples of simulated interactions in order to facilitate understanding of the system and its capabilities	***	***	***	***	***	***	Accept	***	***	***	***	***
c.	Sample data formats and output reports	***	***	***	***	***	***	Accept	***	***	***	***	***
d.	Illustrate and describe all status indicators and information messages.	***	***	***	***	***	***	Accept	***	***	***	***	***
<b>2.8.5</b>	<b>Operating Procedures</b> The vendor shall provide the documentation of system operating procedures that meets the following requirements:												
a.	Provides a detailed description of procedures required to initiate, control, and verify proper system operation	***	***	***	***	***	***	Accept	***	***	***	***	***
b.	Provides procedures that clearly enable the operator to assess the correct flow of system functions (as evidenced by system-generated status and information messages)	***	***	***	***	***	***	Accept	***	***	***	***	***
c.	Provides procedures that clearly enable the operator to intervene the system operations to recover from an abnormal system state	***	***	***	***	***	***	Accept	***	***	***	***	***
d.	Defines and illustrates the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system	***	***	***	***	***	***	Accept	***	***	***	***	***
e.	Defines and illustrates procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved (such information shall be provided for the interaction of the system with other data processing systems or data interchange protocols as well)	***	***	***	***	***	***	Accept	***	***	***	***	***
f.	Provides administrative procedures and off-line operator duties (if any) if they relate to the initiation or termination of system operations, to the assessment of system status, or to the development of an audit trail	***	***	***	***	***	***	Accept	***	***	***	***	***
g.	Supports successful ballot and program installation and control by election officials, provide a detailed work plan or other form of documentation providing a schedule and steps for the software and ballot installation, which includes a table outlining the key dates, events and deliverables	***	***	***	***	***	***	Accept	***	***	***	***	***
h.	Supports diagnostic testing, specify diagnostic tests that may be employed to identify problems in the system, verify the correction of maintenance problems and isolate and diagnose faults from various systems states.	***	***	***	***	***	***	Accept	***	***	***	***	***
<b>2.8.6</b>	<b>Operations Support</b> The vendor shall provide the documentation of system operating procedures that meets the following requirements:												
a.	Defines the procedures required to support system acquisition, installation, and readiness testing. These procedures may be provided by reference, if they are contained either in the system hardware specifications, or in other vendor documentation	***	***	***	***	***	***	Accept	***	***	***	***	***
b.	Describes procedures for providing technical support, system maintenance and correction of defects, and for incorporating hardware upgrades and new software releases.	***	***	***	***	***	***	Accept	***	***	***	***	***
<b>2.8.7</b>	<b>Appendices</b>												

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
	<p>The vendor may provide descriptive material and data supplementing the various sections of the body of the System Operations Manual. The content and arrangement of appendices shall be at the discretion of the vendor. Topics recommended for amplification or treatment in appendix form include:</p> <p>Glossary: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer operations.</p> <p>References: A list of references to all vendor documents and to other sources related to the operation of the system</p> <p>Detailed Examples: Detailed scenarios that outline correct system responses to faulty operator input; Alternative procedures may be specified depending on the system state</p> <p>Manufacturer's Recommended Security Procedures: This appendix shall contain the security procedures that are to be executed by the system operator.</p>												
2.9	<b>System Maintenance Procedures</b>												
	The system maintenance procedures shall provide information in sufficient detail to support election workers, information systems personnel, or maintenance personnel in the adjustment or removal and replacement of components or modules in the field. Technical documentation needed solely to support the repair of defective components or modules ordinarily done by the manufacturer or software developer is not required.	***	***	***	***	***	***	***	Accept	***	***	***	***
	Recommended service actions to correct malfunctions or problems shall be discussed , along with personnel and expertise required to repair and maintain the system; and equipment, materials, and facilities needed for proper maintenance. This manual shall include the sections listed below.	***	***	***	***	***	***	***	Accept	***	***	***	***
2.9.1	<b>Introduction</b>												
	The vendor shall describe the structure and function of the equipment (and related software) for election preparation, programming, vote recording, tabulation, and reporting in sufficient detail to provide an overview of the system for maintenance, and for identification of faulty hardware or software. The description includes a concept of operations that fully describes such items as:	***	***	***	***	***	***	***	Accept	***	***	***	***
a.	The electrical and mechanical functions of the equipment	***	***	***	***	***	***	***	Accept	***	***	***	***
b.	How the processes of ballot handling and reading are performed (paper-based systems)	***	***	***	***	***	***	***	Accept	***	***	***	***
c.	How vote selection and casting of the ballot (DRE systems)	***	***	***	***	***	***	***	Accept	***	***	***	***
d.	How transmission of data over a network (DRE systems, where applicable)	***	***	***	***	***	***	***	Accept	***	***	***	***
e.	How data handling in the processor and memory units	***	***	***	***	***	***	***	Accept	***	***	***	***
f.	How data outputs are initiated and controlled	***	***	***	***	***	***	***	Accept	***	***	***	***
g.	How power is converted or conditioned	***	***	***	***	***	***	***	Accept	***	***	***	***
h.	How test and diagnostic information is acquired and used	***	***	***	***	***	***	***	Accept	***	***	***	***
2.9.2	<b>Maintenance Procedures</b>												

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
	The vendor shall describe preventative and corrective, maintenance procedures for hardware and software.	***	***	***	***	***	***	***	Accept	***	***	***	***
<b>2.9.2.1</b>	<b>Preventative Maintenance Procedures</b> The vendor shall identify and describe:												
a.	All required and recommended preventive maintenance tasks, including software tasks such as software backup, database performance analysis, and database tuning	***	***	***	***	***	***	***	Accept	***	***	***	***
b.	Number and skill levels of personnel required for each task	***	***	***	***	***	***	***	Accept	***	***	***	***
c.	Parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance	***	***	***	***	***	***	***	Accept	***	***	***	***
d.	Any maintenance tasks that must be coordinated with the vendor or a third party (such as coordination that may be needed for off-the-shelf items used in the system).	***	***	***	***	***	***	***	Accept	***	***	***	***
<b>2.9.2.2</b>	<b>Corrective Maintenance Procedures</b>												
	The vendor shall provide fault detection, fault isolation, correction procedures, and logic diagrams for all operational abnormalities identified by design analysis and operating experience.	***	***	***	***	***	***	***	Accept	***	***	***	***
	The vendor shall identify specific procedures to be used in diagnosing and correcting problems in the system hardware (or user-controlled software). Descriptions shall include:	***	***	***	***	***	***	***	Accept	***	***	***	***
a.	Steps to replace failed or deficient equipment	***	***	***	***	***	***	***	Accept	***	***	***	***
b.	Steps to correct deficiencies or faulty operations in software	***	***	***	***	***	***	***	Accept	***	***	***	***
c.	Modifications that are necessary to coordinate any modified or upgraded software with other software modules	***	***	***	***	***	***	***	Accept	***	***	***	***
d.	The number and skill levels of personnel needed to accomplish each procedure	***	***	***	***	***	***	***	Accept	***	***	***	***
e.	Special maintenance equipment, parts, supplies, or other resources needed to accomplish each procedure	***	***	***	***	***	***	***	Accept	***	***	***	***
f.	Any coordination required with the vendor, or other party for off the shelf items.	***	***	***	***	***	***	***	Accept	***	***	***	***
<b>2.9.3</b>	<b>Maintenance Equipment</b>												
	The vendor shall identify and describe any special purpose tests or maintenance equipment recommended for fault isolation and diagnostic purposes.	***	***	***	***	***	***	***	Accept	***	***	***	***
<b>2.9.4</b>	<b>Parts and Materials</b>												
	The vendor shall provide detailed documentation of parts and materials needed to operate and maintain the system. Additional requirements apply for paper based systems.	***	***	***	***	***	***	***	Accept	***	***	***	***
<b>2.9.4.1</b>	<b>Common Standards</b>												
	The vendor shall provide a complete list of approved parts and materials needed for maintenance. This list shall contain sufficient descriptive information to identify all parts by:	***	***	***	***	***	***	***	Accept	***	***	***	***
a.	Type	***	***	***	***	***	***	***	Accept	***	***	***	***
b.	Size	***	***	***	***	***	***	***	Accept	***	***	***	***
c.	Value or range	***	***	***	***	***	***	***	Accept	***	***	***	***
d.	Manufacturer's designation	***	***	***	***	***	***	***	Accept	***	***	***	***
e.	Individual quantities needed	***	***	***	***	***	***	***	Accept	***	***	***	***

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
f.	Source from which they may be obtained	***	***	***	***	***	***	***	Accept	***	***	***	***
<b>2.9.4.2</b>	<b>Paper-Based Systems</b>												
	For marking devices manufactured by multiple external sources, the vendor shall provide a listing of sources and model numbers that are compatible with the system.	***	***	***	***	***	***	***	Accept	***	***	***	***
	The TDP shall specify the required paper stock, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size and location of punch or mark fields used for vote response fields and to identify unique ballot formats, placement of alignment marks, ink for printing, and folding and bleed-through limitations for preparation of ballots that are compatible with the system	***	***	***	***	***	***	***	Accept	***	***	***	***
<b>2.9.5</b>	<b>Maintenance Facilities and Support</b>												
	The vendor shall identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance. In addition, vendors shall specify the assumptions made with regard to any parameters that impact the mean time to repair.	***	***	***	***	***	***	***	Accept	***	***	***	***
a.	Recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation	***	***	***	***	***	***	***	Accept	***	***	***	***
b.	Recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation	***	***	***	***	***	***	***	Accept	***	***	***	***
c.	Organizational affiliation (i.e., jurisdiction, vendor) of qualified maintenance personnel.	***	***	***	***	***	***	***	Accept	***	***	***	***
<b>2.9.6</b>	<b>Appendices</b> The vendor may provide descriptive material and data supplementing the various sections of the body of the System Maintenance Manual. The content and arrangement of appendices shall be at the discretion of the vendor. Topics recommended for amplification or treatment in appendices include: Glossary: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer maintenance. References: A list of references to all vendor documents and to other sources related to the maintenance of the system Detailed Examples: Detailed scenarios that outline correct system responses to every conceivable faulty operator input; alternative procedures may be specified depending on the system state Maintenance and Security Procedures: This appendix shall contain technical illustrations and schematic representations of electronic circuits unique to the system.												
<b>2.10</b>	<b>Personnel Deployment and Training Requirements</b>												
	Verify that the vendor has described the personnel resources and training required for a jurisdiction to operate and maintain the system.	***	***	***	***	***	***	***	Accept	***	***	***	***
<b>2.10.1</b>	<b>Personnel</b> The vendor shall specify the number of personnel and skill levels required to perform each of the following functions:												

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
a.	Pre-election or election preparation functions	***	***	***	***	***	***	***	***	Accept	***	***	***
b.	System operations for voting system functions performed at the polling place	***	***	***	***	***	***	***	***	Accept	***	***	***
c.	System operations for voting system functions performed at the central count facility	***	***	***	***	***	***	***	***	Accept	***	***	***
d.	Preventive maintenance tasks	***	***	***	***	***	***	***	***	Accept	***	***	***
e.	Diagnosis of faulty hardware or software	***	***	***	***	***	***	***	***	Accept	***	***	***
f.	Corrective maintenance tasks	***	***	***	***	***	***	***	***	Accept	***	***	***
g.	Test corrected problems.	***	***	***	***	***	***	***	***	Accept	***	***	***
	A description identifies functions that may be carried out by user personnel, and those that must be performed by vendor personnel.	***	***	***	***	***	***	***	***	Accept	***	***	***
<b>2.10.2</b>	<b>Training</b> The vendor shall specify the requirements for orientation and training of the following personnel:												
a.	Poll workers supporting polling place operations	***	***	***	***	***	***	***	***	Accept	***	***	***
b.	System support personnel involved in election programming	***	***	***	***	***	***	***	***	Accept	***	***	***
c.	User system maintenance technicians	***	***	***	***	***	***	***	***	Accept	***	***	***
d.	Network/system administration personnel (if a network is used)	***	***	***	***	***	***	***	***	Accept	***	***	***
e.	Data personnel	***	***	***	***	***	***	***	***	Accept	***	***	***
f.	Vendor personnel.	***	***	***	***	***	***	***	***	Accept	***	***	***
<b>2.11</b>	<b>Configuration Management Plan</b>												
	Vendors shall submit a Configuration Management Plan that addresses the configuration management requirements of Volume I, Section 8. This plan shall describe all policies, processes, and procedures employed by the vendor to carry out these requirements. The Configuration Management Plan shall contain the sections identified below.	***	***	***	***	***	***	***	***	Accept	***	***	
<b>2.11.1</b>	<b>Configuration Management Policy</b>												
	The vendor shall provide a description of its organizational policies for configuration management, per Volume I, Section 8.2 of the Standards. These requirements pertain to:	***	***	***	***	***	***	***	***	Accept	***	***	
a.	Scope and nature of configuration management program activities	***	***	***	***	***	***	***	***	Accept	***	***	
b.	Breadth of application of vendor's policy and practices to the voting system.	***	***	***	***	***	***	***	***	Accept	***	***	
<b>2.11.2</b>	<b>Configuration Identification</b>												
	The vendor shall provide a description of the procedures and naming conventions used to address the specific requirements of Volume I, Section 8.3. These requirements pertain to:	***	***	***	***	***	***	***	***	Accept	***	***	
a.	Classifying configuration items into categories and subcategories	***	***	***	***	***	***	***	***	Accept	***	***	
b.	Uniquely numbering or otherwise identifying configuration items	***	***	***	***	***	***	***	***	Accept	***	***	
c.	Naming configuration items.	***	***	***	***	***	***	***	***	Accept	***	***	
<b>2.11.3</b>	<b>Baseline, Promotion, and Demotion Procedures</b>												
	The vendor shall provide a description of the procedures and naming conventions used to address the specific requirements of Volume I, Section 8.4. These requirements pertain to:	***	***	***	***	***	***	***	***	Accept	***	***	
a.	Establishing a particular instance of a system component as the	***	***	***	***	***	***	***	***	Accept	***	***	

<b>VSS &amp; VVSG</b>	<b>Volume 2 Testing Requirement-Section 2 Technical Data Package</b>	<b>2.2</b>	<b>2.3</b>	<b>2.4</b>	<b>2.5</b>	<b>2.6</b>	<b>2.7</b>	<b>2.8</b>	<b>2.9</b>	<b>2.10</b>	<b>2.11</b>	<b>2.12</b>	<b>2.13</b>
	starting baseline												
b.	Promoting subsequent instances of a component to baseline throughout the system development process for the first complete version of the system submitted for testing	***	***	***	***	***	***	***	***	***	Accept	***	***
c.	Promoting subsequent instances of a component to baseline status as the component is maintained throughout its life cycle	***	***	***	***	***	***	***	***	***	Accept	***	***
<b>2.11.4 Configuration Control Procedures</b>													
	The vendor shall provide a description of the procedures used by the vendor to approve and implement changes to a configuration item to prevent unauthorized additions, changes, or deletions to address the specific requirements of Volume I, Section 8.5 of the standards. These requirements pertain to:	***	***	***	***	***	***	***	***	***	Accept	***	***
a.	Developing and maintaining internally developed items	***	***	***	***	***	***	***	***	***	Accept	***	***
b.	Developing and maintaining third-party items	***	***	***	***	***	***	***	***	***	Accept	***	***
c.	Resolving internally identified defects	***	***	***	***	***	***	***	***	***	Accept	***	***
d.	Resolving externally identified and reported defects.	***	***	***	***	***	***	***	***	***	Accept	***	***
<b>2.11.5 Release Process</b>													
	The vendor shall provide a description of the contents of a system release, the procedures and related conventions by which the vendor installs, transfers, or migrates the system to ITAs and customers to address the specific requirements of Volume I, Section 8.6. These requirements pertain to:	***	***	***	***	***	***	***	***	***	Accept	***	***
a.	A first release of the system to an accredited test lab	***	***	***	***	***	***	***	***	***	Accept	***	***
b.	A subsequent maintenance or upgrade releases of a system or component to an accredited test lab	***	***	***	***	***	***	***	***	***	Accept	***	***
c.	The initial delivery and installation of the system to a customer	***	***	***	***	***	***	***	***	***	Accept	***	***
d.	The subsequent maintenance or upgrade release of a system or component to a customer.	***	***	***	***	***	***	***	***	***	Accept	***	***
<b>2.11.6 Configuration Audits</b>													
	The vendor shall provide a description of the procedures and related conventions for the two audits required by Volume I, Section 8.7. These requirements pertain to:	***	***	***	***	***	***	***	***	***	Accept	***	***
a.	Physical configuration audit that verifies the voting system components submitted for qualification to the vendor's technical documentation	***	***	***	***	***	***	***	***	***	Accept	***	***
b.	Functional configuration audit that verifies the system performs all the functions described in the system documentation.	***	***	***	***	***	***	***	***	***	Accept	***	***
<b>2.11.7 Configuration Management Resources</b>													
	The vendor shall provide a description of the procedures and related conventions for maintaining information about configuration management tools required by Vol. I, Sect. 8.9. These requirements pertain to:	***	***	***	***	***	***	***	***	***	Accept	***	***
a.	Specific tools used, current version, and operating environment	***	***	***	***	***	***	***	***	***	Accept	***	***
b.	Physical location of the tools, including designation of computer directories and files	***	***	***	***	***	***	***	***	***	Accept	***	***
c.	Procedures and training materials for using the tools.	***	***	***	***	***	***	***	***	***	Accept	***	***
<b>2.12 Quality Assurance Program</b>													

VSS & VVSG	Volume 2 Testing Requirement-Section 2 Technical Data Package	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	2.11	2.12	2.13
	The vendor shall submit a Quality Assurance Program that addresses the quality assurance requirements of Volume I, Section 7. This plan describes all policies, processes and procedures employed by the vendor to ensure the overall quality of the system for its initial development, release and for subsequent modifications and releases. The Quality Assurance Program shall, at a minimum, address the topics indicated below.	***	***	***	***	***	***	***	***	***	***	Accept	***
<b>2.12.1</b>	<b>Quality Assurance Policy</b>												
	The vendor shall provide a description of its organizational policies for quality assurance, including:	***	***	***	***	***	***	***	***	***	***	Accept	***
a.	Scope and nature of QA activities	***	***	***	***	***	***	***	***	***	***	Accept	***
b.	Breadth of application of vendor's policy and practices to the voting system.	***	***	***	***	***	***	***	***	***	***	Accept	***
<b>2.12.2</b>	<b>Parts &amp; Materials Special Tests and Examinations</b>												
	The vendor shall provide a description of its practices for parts and materials tests and examinations that meet the requirements of Volume I, Section 7.5.	***	***	***	***	***	***	***	***	***	***	Accept	***
<b>2.12.3</b>	<b>Quality Conformance Inspections</b>												
	The vendor shall provide a description of its practices for quality conformance inspections that meet the requirements of Volume I, Section 7.6 of the Standards. For each test performed , the record of tests provided shall include:	***	***	***	***	***	***	***	***	***	***	Accept	***
a.	Test location	***	***	***	***	***	***	***	***	***	***	Accept	***
b.	Test date	***	***	***	***	***	***	***	***	***	***	Accept	***
c.	Tester name	***	***	***	***	***	***	***	***	***	***	Accept	***
d.	Test outcomes.	***	***	***	***	***	***	***	***	***	***	Accept	***
<b>2.12.4</b>	<b>Documentation</b>												
	The vendor shall provide a description of its practices for documentation of the system and system development process that meet the requirements of Volume I, Section. 7.7 of the Standards.	***	***	***	***	***	***	***	***	***	***	Accept	***
<b>2.13</b>	<b>System Change Notes</b>												
	Vendors submitting a system for testing that has been tested previously by the test authority and issued a qualification number, the vendor shall submit system change notes. The system change notes shall include the following information:	***	***	***	***	***	***	***	***	***	***	***	Accept
a.	A summary description of the nature, scope and reasons for each change	***	***	***	***	***	***	***	***	***	***	***	Accept
b.	A listing of the specific changes made, citing the specific system configuration items changed and providing detailed references to the sections of documentation changed	***	***	***	***	***	***	***	***	***	***	***	Accept
c.	The specific sections of the documentation that are changed (or complete revised documents, if more suitable to address a large number of changes)	***	***	***	***	***	***	***	***	***	***	***	Accept
d.	Documentation of the test plan and procedures executed by the vendor for testing the individual changes and the system as a whole, and records of test results.	***	***	***	***	***	***	***	***	***	***	***	Accept

## 7.4 Appendix D: FCA Testing

Test results identified in Appendix D include the M100, the addition of an EMS network LAN, the modifications from the certified **ESSUnity3200** and a system level regression test of the complete Unity 3.2.1.0 voting system.

### 7.4.1 FCA Functional System Level, Accessibility, Maintainability, Accuracy & Reliability Testing

These test results reference the testing performed by SysTest Labs in the Unity 4.0.0.0 certification and the Regression System Level Test Case executed by iBeta.

#### 7.4.1.1 Reuse Functional System Level, Accessibility, Maintainability, Accuracy & Reliability Test Results

The test results and test configuration of the testing by SysTest are contained in the Summary Report of testing performed by SysTest. The VSS 2000 requirements associated with this testing are identified Appendix H Amended Test Plan.

#### 7.4.1.2 Regression System Level Test Result

iBeta conducted testing on the system configuration cross referenced in the test method below. Specific software and firmware builds for each test execution were recorded in the PCA Configuration as identified in the test case document.

Date	Test Result	Issues Opened	Issues Closed	Notes
10/12/2009	Reject	# 80, 81, 82, 83		<b>Scenario 1 Rev. 00</b> Security discrepancies
3/20/2010	Reject	# 136 , 137, 138, 140	# 80, 81, 82, 83	<b>Scenario 1 Rev. 01</b>
3/20/2010	Accept			<b>Scenario 2 Rev. 01</b>
4/1/2010	Reject	# 144	# 9	<b>Scenario 3 Rev. 01</b>
4/2/2010	Accept			<b>Scenario 5 Rev. 01</b>
4/5/2010	Reject	# 146, 156	# 20	<b>Scenario 4 Rev. 01</b> - Discrepancy # 20 was found at SysTest Labs and tested by iBeta. Discrepancy #20 was closed however; a new discrepancy was opened.
4/22/2010	Halted			<b>Scenario 1 REV 02</b> – M650 “Channel D” required maintenance.
4/26/2010	Reject	# 140	# 137, 138	<b>Scenario 1 REV 02</b> -continued execution of Scenario 1 REV 02 after maintenance Disc #136 was closed via documentation 4/12/2010.
5/3/2010	Accept		# 156	<b>Scenario 4 REV 02</b> <b>Discrepancy 146</b> was addressed by documentation and closed 4 /22/2010, no functional testing was required.
8/4/2010	Accept	#103, 174	#144	<b>Scenario 3 Rev. 02</b> When Disc #136 was closed discrepancy #103 was reopened. Disc #140 was closed with documentation 5/4/2010
8/6/2010	Accept		#174, 103	<b>Scenario 1 REV 03</b> Created a Func Rev 00 to test in conjunction with S1Rev03 due to the changes in documentation. #103 and 174 were documentation discrepancies found during Security Documentation review. The document changes required functional verification. Was put on hold on 8/10 awaiting documentation. Testing continued on 9/27.
11/12/2010	Accept	#188	# 183	<b>Scenario 6 REV 00</b> Created S6 "M100 Audit Log ENH19171" Tested and closed # 183 (BUG19781) <b>Discrepancy 188</b> was observed in setting up the test

				environment but it was not relevant to the Scenario 6 test. The test was accepted. A new discrepancy was written which will require a new test case.
--	--	--	--	--

While documentation discrepancies may be encountered in testing they do not result in the rejection of a functional test. Identified issues are found in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#).

Method Detail	Reuse of SysTest System Level Test Method	Regression System Level Test Method
Test Case Name	Reuse of SysTest System Level Test Method	Regression System Level Test Case
Scope - identifies the type of test	Reuse System Level : SysTest Unity v.4.0.0.0 Test Cases applicable to the scope of Unity 3.2.1.0: Readiness, Functional, Maintainability, GEN01, GEN02, GEN02 PA, GEN03, PRI01, PRI01 PP, PRI02, 40HTEST1, Ohio Test, 40HTEST3, 40HTEST4, 40HTEST5, 3000 Precincts, Error Recovery, and Electrical Supply	<p>The scope is to test, create and tally the election on a Windows 2003 server based network (multiple PCs) set up, and a regression system level test incorporating validations of a substantial portion of the VSS 2002, <a href="#">VVSG 2005 v.1:2.1.6</a> required and vendor identified functionality for the Unity 3.2.1.0 voting system.</p> <p>Pre-vote: Create a Pick-a-Party Primary election; prepare election media and paper ballots in EDM, ESSIM and HPM; import into AIMS.</p> <p>Vote: Vote Election Day hand &amp; machine marked paper ballots (VAT:A100 &amp; A200); precinct scanning (DS200 and M100)</p> <p>Post Vote: Write election results (DS200 and M100); scan absentee hand marked and VAT marked ballots (M650 central scanner); consolidate absentee &amp; Election Day votes into ERM for tallying and reporting.</p> <p>Testing includes validation of measurable performance including accuracy, processing rate, and ballot format handling capability, incorporating:</p> <p>The test case will have 6 scenarios. All Scenarios are using the same election data. At times there are some different settings for Scenarios 2 – 6 those are listed below.</p>
Test Objective	ES&S has petitioned the EAC for reuse of the applicable components in scope for Unity 3.2.1.0 from the SysTest testing of the Unity v.4.0.0.0 certification test effort. Determination of reuse of test results for functional, system level, usability, and accessibility testing performed by SysTest validating the VSS 2002 required and ES&S identified functionality for the Unity 3.2.1.0 voting system is identified in Appendix C.	<p>The objective is to validate the ability to store and tally an election on a Windows 2003 server based network configuration, and:</p> <ul style="list-style-type: none"> <li>- Accurately and securely create paper English and Spanish visual and audio ballots for a pick-a-party primary election;</li> <li>- Create and install election specific media for the VAT and DS200, M100 and M650;</li> <li>- Independently and securely vote audio and visual ballots with mobility and non-mobility restrictions;</li> <li>- Count and report the results and;</li> </ul> <p>Validate identified discrepancies:</p> <ul style="list-style-type: none"> <li>- Discrepancy #7 - M100 accepted ballots that were copied from un-voted original ballots on a laser color copier printer</li> <li>- Discrepancy #9 - Create 4 groups (1- M100, 2- DS200, 3 - M650, 4 - M650 A). After creating the groups go back and switch the location of the M650 group and the M100 group. (Scenario 3)</li> <li>- Discrepancy #20 - In HPM when the System Type is set to the "Mixed" option in an election that is all Scanner (M100, DS200 &amp; M650), an error is generated in ERM when creating results database</li> <li>- Discrepancy #20 (BUG13633) - In HPM when the System Type is set to the "Central Count" option in an election that is only using an M650 Central Scanner, an error is generated in ERM when creating results database.</li> </ul>

<b>Method Detail</b>	<b>Reuse of SysTest System Level Test Method</b>	<b>Regression System Level Test Method</b>
		<ul style="list-style-type: none"> <li>-Event Sever logging (Scenario 2)</li> <li>- Audit Logs M100 ONLY (Scenario 6- RFI 2009-04)</li> </ul>
Test Variables: Voting Variations (as supported by the voting system)	Determination by the EAC of the reuse of SysTest testing, test results and test reporting for Ballot-on-Demand (BOD), VAT and tabulators (M100), for ESSUNITY3200 from the SysTest testing of the Unity v.4.0.0.0 certification test effort.	<p>In Scope for Unity 3.2.1.0:</p> <p>Wisconsin Open Pick-a-Party Primary comprising:</p> <ul style="list-style-type: none"> <li>- An 14 inch combined paper ballot containing Dem, Rep &amp; Non-Partisan selections, with ovals on the right side</li> <li>- 1 Polling Place</li> <li>- 2 Ballot Styles comprising: Ballot Style 1: 1000, 2000, 3000-02, Ballot Style 2: 3000-01</li> <li>- 3 Precincts (1000, 2000, 3000) splits (3000-01, 3000-02)</li> <li>- 2 Partisan, 1 Non-Partisan, 1 Referendum Contests &amp; a Party Selection</li> </ul> <p>Discrepancy #20 - In HPM select "Mixed" to read in all types of election media into ERM.</p> <p>Election Day voting (VAT, M100 &amp; DS200), Absentee Voting (M650)</p> <p>Vote for 1, Vote for N of M, Write-in votes (all contests)</p> <p>Assistive Devices (AT paddles, tactiley discernible keypad, Audio\Visual ballots)</p> <p>Multi-lingual Audio &amp; Visual Ballots (English &amp; Spanish)</p> <ul style="list-style-type: none"> <li>- Create all Spanish translations in EDM: modify Democrat part WAV files for Spanish and English &amp; create WAV audio file recorded in AIMS</li> <li>- VAT alerts (set in AIMS) ballots Overvoted and Undervoted</li> <li>- DS200 and M100 Ballot Control Options (HPM): Query: Overvotes, Crossover, and Blank ballots; Reject: Unreadable marks; Accept: undervote.</li> <li>- M100 - Diverter Installed to divert Blank and Write-in ballots in ballot box</li> </ul>
A description of the voting system type and the operational environment	See Appendix C	The Unity 3.2.1.0 EMS includes a Windows 2003 server based network.
VSS 2002 vol. 1	2.2.1 thru 2.2.9, 2.2.11 thru 2.5.3.2, 2.5.4, 3.2.4 thru 3.2.4.2.1, 3.2.4.2.3, 3.2.4.2.5, 3.2.4.2.6, 3.2.5 thru 3.2.6.1.2, 3.2.7 thru 3.2.8.2 HAVA a thru c2 RFI: 2007-02, 2007-04, 2007-06, 2008-04, 2008-07, 2008-12	<p>2.2.1 thru 2.2.9, 2.3.1.1 thru 2.5.3.2 , (DRE requirements applicable to VAT excluding vote storage) 3.2.4.2.5, 3.2.4.2.6, 3.2.5.1.3 a thru d.4, 3.2.6.1.1, 3.2.8 thru 3.2.8.2</p> <p>HAVA a thru c2</p> <p>VVSG vol. 1: 2.1.6</p> <p>RFI: 2007-04, 2007-06, 2008-04, 2008-07, 2008-12</p>
VSS 2002 vol. 2	6.2, 6.2.1, 6.2.2, 6.3, 6.4, 6.4.1, 6.5, 6.6, 6.7 RFI: 2007-06, 2008-07, 2008-12	6.2, 6.2.1, 6.2.2, 6.3, 6.4, 6.4.1 , 6.5, 6.6, 6.7 RFI: 2007-06, 2008-07, 2008-12
Hardware, Software voting system configuration and test location	Determination by the EAC of the reuse of SysTest testing. Configuration of SysTest See Appendix C	<p>EMS Software:</p> <p>EMS Ballot Preparation SW: Audit Manager (AM), Election Data Manager (EDM), ES&amp;S Image Manager (ESSIM), Hardware Programming Manager (HPM), AutoMARK Information Management System (AIMS), Election Reporting Manager (ERM), LogMonitor Service</p> <p>Hardware:</p> <ul style="list-style-type: none"> <li>(5) Ballot Marking Device: Voter Assist Terminal (VAT), Models A100 (1) &amp; A200 (4)</li> <li>(1) Precinct Count scanner/tabulator: intElect DS200 (DS200 w/plastic ballot box)</li> <li>(1) Precinct Count scanner/tabulator: intElect DS200 (DS200 w/steel diverter ballot box)</li> </ul>

<b>Method Detail</b>	<b>Reuse of SysTest System Level Test Method</b>	<b>Regression System Level Test Method</b>
		<p>(1) Precinct Count scanner/tabulator: Model 100 (M100 w/ steel ballot box with diverter)  (1) Precinct Count scanner/tabulator: Model 100 (M100 w/ plastic ballot box (containing M100 rails))  (1) Central Count scanner/tabulator: Model 650 (M650)  (1) File Server  (2) PC for Unity and AIMS EMS applications  (2) PCs for ERM  (1) Network Printer  (1) Network hub/switch</p> <p>Test Location: iBeta, 2675 S. Abilene, Aurora, CO 80014</p>
Pre-requisites and preparation for test case execution	See Appendix C	<p>Prior to execution of testing, the following prerequisites must be completed:</p> <ul style="list-style-type: none"> <li>- Record the testers &amp; date</li> <li>- Perform and install witness/trusted build of software/firmware components utilizing ES&amp;S documentation</li> <li>- System has been installed and set up as identified in the user manuals</li> <li>- Gather any necessary materials or manuals (A microphone, PC soundcard and speakers are available/installed to record audio, white and blue blank ballot stock paper)</li> <li>- Ensure customization of the test case template is complete</li> </ul>
Getting Started Checks	See Appendix C	<p><b>Check the voting system to:</b></p> <ul style="list-style-type: none"> <li>- Verify the test environment and system configuration is documented in the PCA Configuration matches the configuration of the system used in the 48 hr. temp &amp; power variation test and vendor described configuration.</li> <li>- Validate installation of the witnessed build</li> <li>- Testers understand that no change shall occur to the test environment without documentation in the test record and the authorization of the project manager.</li> <li>- During testing an operational readiness test will be performed.</li> <li>- The environment is set up with a Windows 2003 server based network. (Configuration is as follows: 1 PC for Unity/AIMS ballot prep. software, 3 PCs for ERM, 1 network printer, 1 file server, Network hub/switch, 1 M100 steel ballot box with a diverter and 1DS200 plastic ballot box-returned from hardware test lab)</li> </ul>
Documentation of Test Data & Test Results	See Appendix C	<p>Test Data:</p> <ul style="list-style-type: none"> <li>- Record all programmed &amp; observed election, ballot &amp; vote data fields and field contents on the corresponding tabs to provide a method to repeat the test</li> <li>- Preserve all tabs for each instance the test is run.</li> </ul> <p>Test Results:</p> <ul style="list-style-type: none"> <li>- Enter Accept/Reject on the Test Steps</li> <li>- In Comments enter any deviations, discrepancies, or notable observations</li> <li>- Log discrepancies on the Discrepancy Report and insert the number in the Comments</li> </ul>
Pre-vote: Ballot Preparation procedures	See Appendix C	<p>Ballot Prep: Verify (RFI: 2007-04, 2008-04, 2008-07)  - Spanish/English, visual/audio ballots (contests, candidates, propositions and associated</p>

Method Detail	Reuse of SysTest System Level Test Method	Regression System Level Test Method
verifications		<p>offices/labels) can be accurately/securely defined with multiple ballot styles, precincts and splits.</p> <p>In EDM change:</p> <ul style="list-style-type: none"> <li>- Ballot Sets/Ballot Style ID - By Precinct</li> <li>- Add a Party - enter: 4 (Order), XVR (ID), 3 (Device), Crossover (Party Name)</li> <li>- Ballots contain partisan races segregated by party and non-partisan races (Dem, Rep, Non-Partisan)</li> <li>- Ballots contain identifying marks (ballot style, precincts/splits)</li> <li>- Ballot &amp; VAT: ovals properly align with candidate names/issues so voters can clearly mark selections; spacing and font size is consistent so there is no preferential voting position</li> <li>- VAT: maximum choices for a single contest are displayed on one page</li> <li>- The election can be accurately/securely imported from Unity 3.2.1.0 into AIMS. (Prerequisite: define and print ballot in Unity 3.2.1.0, before importing into AIMS.)</li> <li>- The AIMS database can be modified, as required, to support the election definition required for VAT operation; and using AIMS Preview function confirm data was imported correctly and ballots are set up correctly.</li> <li>- Election media can be accurately/securely programmed in HPM and AIMS for installation in all voting &amp; tabulating devices. (VAT, DS200, M650)</li> <li>- Verify audit logs for AM, EDM, ESSIM, HPM and AIMS for message IUIimport - Performed full Unity election import.</li> <li>- Verify audit logs for status/error messages: EDM: Minimum password length is 6 characters, District Type Name can not be blank, ESSIM: Please Enter a Style Sheet Name, HPM: Admin password is required</li> <li>- Installation of Election</li> <li>- Insert a blank CF card, turn to ON position and verify system will not boot up without an election definition.</li> <li>- Insert a CF card with an election, turn to ON position and verify self-test is successful and VAT displays "Please Insert Your Ballot"</li> <li>- VAT: Setup; perform maintenance checks: ink cartridge, Battery charge, Install Flash Memory Card, Test VAT operations, Set Admin password, Calibrate, Set 'Maint' password to confirm there are no hardware/software failures</li> <li>- DS200, M100 &amp; M650: Setup &amp; install election; set Date &amp; Time; and perform readiness tests</li> <li>- HPM System Type is set to "Both"</li> </ul> <p><b>Scenario 4:</b> HPM System Type is set to "Mixed" Create 2 M100 PCMCIA cards by selecting the OMNI-PARALLEL Drive (ENH17725 Disc #107) and OMNI-USB Drive. The OMNI-PARALLEL PCMCIA card will be used on election day, the OMNI-US will be used only as an election day backup card.</p> <p><b>Scenario 5:</b> HPM System Type is set to "Central Count" for the M650 tally only.</p>
Pre-vote: Ballot Preparation Security	See Appendix C	<p>Ballot Prep:</p> <ul style="list-style-type: none"> <li>- Security access controls limit or detect access to critical systems and the loss of system integrity,</li> </ul>

Method Detail	Reuse of SysTest System Level Test Method	Regression System Level Test Method
		<p>availability, confidentiality &amp; accountability,</p> <ul style="list-style-type: none"> <li>- ID and password can be defined for EDM, ESSIM &amp; AIMS.</li> </ul> <p>(Use newly created id/password during Pre-Vote activities.)</p> <ul style="list-style-type: none"> <li>- Password required to start AIMS</li> <li>- Password required to access EDM</li> <li>- Verify access is permitted and denied without proper credentials for each of the systems</li> <li>- Functions are only executable in the intended manner, order &amp; under intended conditions</li> <li>- Prevents execution of functions if preconditions weren't met</li> <li>- Implemented restrictions on controlled functions</li> <li>- Documentation of mandatory administrative procedures.</li> </ul> <p>COTS</p> <ul style="list-style-type: none"> <li>- Authentication is configured on the local terminal &amp; external connection devices,</li> <li>- Operating systems are enabled for all session &amp; connection openings, &amp; closings, all process executions &amp; terminations &amp; for the alteration or detection of any memory or file object</li> <li>- Configure the system to only execute intended &amp; needed processes during the execution election software. Processes are halted until termination of critical system processes (such as audit).</li> </ul>
Readiness Testing and Poll Verification	See Appendix C	<p>Readiness Testing: Verification that:</p> <p>VAT: Proper election has been installed: all buttons, printers and screen function correctly; matching version is displayed; and a ballot can be marked in test mode.</p> <ul style="list-style-type: none"> <li>- Review audit logs to confirm readiness for VAT</li> <li>- Prevents execution of functions if preconditions weren't met</li> </ul> <p>VAT: Verify A password is required to access the System Maint menu</p> <p>DS200, M100 &amp; M650: Readiness testing automatically incorporated into Opening the Polls; Election name, equipment identification, polling place &amp; ballot format and matching version is displayed or printed on initial state report and/or zero count report; confirmation that there are no hardware/software failures ; and device is ready to be activated to accept votes. Perform readiness testing according to VSS requirements</p> <ul style="list-style-type: none"> <li>- Obtain status, data reports, audit logs and other artifacts to confirm readiness</li> <li>- Attempt to open polls with test totals. Verify a visual screen warning is provided if memory locations contain votes, and the reports/audit log contain a time-stamp record of the status of the votes/results memory and disk storage locations. If a unit or system contains a non-zero counter, a warning message is provided, along with corrective actions to resolve the votes. The unit is disabled until type of resolution is selected. Clear totals on the M100 and the DS200 only.</li> </ul> <p>DS200: Verify A password is required to access the Admin menu and to reopen polls</p> <p>M100: Verify A password is required to reopen the polls and access additional reports</p> <p>Read in the M650 test results into ERM. Do not clear</p>

Method Detail	Reuse of SysTest System Level Test Method	Regression System Level Test Method
		<p>totals at this time.</p> <p><b>Discrepancy 7:</b> counterfeit (copies of valid ballots) ballots are rejected by the M100, verify:</p> <ul style="list-style-type: none"> <li>•an error message stating "BALLOT READ ERROR-Please See Election Official" is displayed on the screen</li> <li>•a generated audio beep for at least five seconds or as long as the ballot has not been removed is heard.</li> </ul> <p><b>S6 - Discrepancy 183 (BUG19781)</b> M100 " test" totals are not cleared when selecting the No (do not clear) option</p>
Pre- vote: Opening the Polls Verification	See Appendix C	<p>Precinct Count:</p> <ul style="list-style-type: none"> <li>- DS200 select 'Open Polls'. Zero report will automatically print, an internal test will be performed and results will display. If test is unsuccessful, DS200 will automatically shut down; If successful will display "Please Insert Your Ballot" message</li> </ul> <p>Paper based: Verify VAT, M100 &amp; DS200 are ready for use:</p> <ul style="list-style-type: none"> <li>- VAT &amp; DS200 display "Please Insert Your Ballot" message.</li> <li>- Any failures provide a message for resolution</li> <li>- VAT holds the ballot securely</li> <li>- DS200 &amp; M100 do not contain a frame or fixture for ballot marking</li> <li>- DS200 is attached to a custom DS200 plastic or metal ballot box; with locks and separate compartments; slots prevent unauthorized ballot insertion. Write-ins will be marked with a red circle to indicate review is necessary</li> <li>- M100 is attached to a custom M100 metal ballot box; with locks and separate compartments; slots prevent unauthorized ballot insertion.</li> <li>- VAT security seals are checked: compact flash compartment, top cover &amp; ink compartment</li> </ul>
Voting: Ballot Activation and Casting Verifications	See Appendix C	<p>Verify (RFI: 2007-06, 2008-12) <b>VAT, M100 &amp; DS200</b></p> <p>Protects secrecy of ballot/vote</p> <ul style="list-style-type: none"> <li>- Voter can make selections based on ballot programming &amp; indicate selection, cancellation, &amp; non-selection (undervotes)</li> <li>- Gives feedback &amp; an opportunity to correct or accept, before the ballot is counted</li> <li>- Functions are only executable in the intended manner, order &amp; under intended conditions</li> <li>- Prevents execution of functions if preconditions weren't met</li> </ul> <p><b>VAT</b></p> <ul style="list-style-type: none"> <li>- Control of ballot (single ballot cast per vote session) and content of ballot is restricted to the eligible voter</li> <li>- Correct ballot is presented (language, audio/visual, precinct/split)</li> <li>- Party affiliation content is controlled/activated via the "Party Preference"</li> <li>- Touching an area outside the identified selection box does not mark the ballot or display external information</li> <li>- Provides all displays, instructions, messages, alerts and status in multilingual audio &amp; visual displays</li> <li>- Voters are able to edit and review write-ins. # of write-ins match Vote For.</li> <li>- Audio voting provides repeat functionality &amp; volume</li> </ul>

Method Detail	Reuse of SysTest System Level Test Method	Regression System Level Test Method
		<p>control</p> <ul style="list-style-type: none"> <li>- Voter is allowed to mark the ballot, in any combination, or return it without marking (blank)</li> <li>- Overvote and Undervote provides alerts, with overvotes prevented</li> <li>- Summary screen is provided to signify end of candidate/measures and provides instructions to review/change selections prior to ballot marking</li> <li>- Verify alert of selection's complete, ballot is being marked, and to take completed ballot to tabulator</li> </ul> <p><b>DS200 &amp; M100</b></p> <ul style="list-style-type: none"> <li>- Alert successful/unsuccessful storage of cast ballot; provide review &amp; instruction to resolve unsuccessful casting (Query: Overvotes, Crossover, and Blank ballots; Reject: Unreadable marks; Accept: undervote.</li> <li>- Increments the ballot counter for successfully cast ballots</li> <li>- Print Precinct and Status reports to compare to vote data to verify actual votes cast is correct &amp; undervotes/overvotes are counted separately</li> <li>- Access to voted ballot is prevented until after polls close (locked ballot box)</li> </ul> <p><b>M100:</b></p> <ul style="list-style-type: none"> <li>- External printer is connected, becoming the default printer for reports</li> <li>- Diverter Installed to divert Blank and Write-in ballots in ballot box</li> <li>- <b>Clearinghouse CT 7/1/07:</b> Verify that simultaneously pressing 2 buttons will not cause the polls to close</li> <li>- <b>Discrepancy 7:</b> photocopied ballots are rejected by the M100</li> <li>• an error message stating "BALLOT READ ERROR- Please See Election Official" is displayed on the screen</li> <li>• a generated audio beep for at least five seconds or as long as the ballot has not been removed is heard.</li> </ul>
Voting: Voting System Integrity, System Audit, Errors & Status Indicators	See Appendix C	<p>The system audit provides a time stamped, always available, report of normal/abnormal events that can't be turned off when the system is in operating mode.</p> <ul style="list-style-type: none"> <li>- Maintain accurate and complete audit records; verify at various points (After poll open; vote query, reject &amp; accept: any abnormal event encountered in testing; poll close)</li> <li>- Self-tests and diagnostic messages for the hardware will be verified at poll open/close points in the test case</li> <li>- Status messages are part of the real time audit record.</li> <li>- Critical status messages requiring operator intervention shall use clear indicators or text</li> </ul> <p><b>Bug15827</b> Overvoted Write-In ballots are diverted into the correct bin.</p> <p><b>ENH16120/ENH16291/16336</b> message appears when too many votes have been selected (Overvote messages in English and Spanish)</p> <p>Error messages are:</p> <ul style="list-style-type: none"> <li>- Generated, stored &amp; reported as they occur</li> <li>- Errors requiring intervention by the voter or poll worker clearly display issues &amp; action instructions in easily understood text language or with indicators</li> <li>- The text for any numeric codes is contained in the</li> </ul>

<b>Method Detail</b>	<b>Reuse of SysTest System Level Test Method</b>	<b>Regression System Level Test Method</b>
		<p>error or affixed to the inside of the voting system  - Incorrect responses will not lead to irreversible errors.</p>
Post-vote: Closing the Polls	See Appendix C	<p>VAT:  - Turn VAT to 'Off' position &amp; remove FMC to prevent further casting of ballots; verify a voting session cannot be activated.  - Review the audit logs (only available report ) to verify entries are in the proper sequence for operational tests, switching from test to vote modes, ballot printing, audit report access during voting , including complete &amp; accurate error and status messages</p> <p><b>DS200 &amp; M100:</b></p> <ul style="list-style-type: none"> <li>- Attempt to print reports while polls are open; verify this is prohibited.</li> <li>- Close the polls and a Results Report will print preventing further casting of ballots (attempt to scan a ballot without reopening the polls)</li> <li>- Visibly displays the status "Polls Closed"</li> <li>- Internally tests and verifies that the closing procedures have been followed and the device status is normal by preventing report printing or processing vote totals unless polls were properly closed.</li> <li>- Confirm polls cannot be reopened without password</li> <li>- Review the audit log to verify test records exists that verify entries for the proper sequence for operational tests, poll open; vote query, reject &amp; accept: any abnormal event encountered in testing; poll close, including complete &amp; accurate error and status messages</li> <li>- Print Status report, Race Results report, Certification report, Precinct Report Summary, Poll Report Summary and Audit Log report once polls are closed. Ensure undervote &amp; overvote is counted.</li> </ul> <p><b>-ENH16231</b> DS200 audit log enhancements for accessing the Administrative menu (displaying the successful and unsuccessful login attempts).</p> <p><b>- Validate data from USB/PCMCIA is extractable by transmitting results into ERM</b></p> <p><b>Reopen the polls testing:</b></p> <ul style="list-style-type: none"> <li>- Reopen of polls, enter an incorrect and then a correct password</li> <li>- Alert to resume voting or clear votes: select 'resume voting', do not clear votes</li> <li>- Status message "Please insert your ballot" is displayed</li> <li>- Cast a vote and close the polls.</li> <li>- Check audit for proper sequence for operational tests, poll open, vote accept, poll close, reopen, password entry</li> <li>- Verify correct vote totals.</li> </ul> <p><b>Scenario 6:</b></p> <ul style="list-style-type: none"> <li>•<b>ENH19171:</b> An audit log entry displays each time the DS200 powers up.</li> <li>•<b>ENH19171:</b> The Log will display "<b>Ballot Cast</b>" for each ballot that was successfully scanned with a time and date stamp.</li> </ul>
Post-vote: Central Count	See Appendix C	<p>Obtain status, data reports, audit logs and other artifacts to confirm readiness</p> <ul style="list-style-type: none"> <li>- M650: Verify the back door is locked</li> <li>- Votes match predicted votes (absentee)</li> </ul>

Method Detail	Reuse of SysTest System Level Test Method	Regression System Level Test Method
		<ul style="list-style-type: none"> <li>- Geographic reports of votes; each contest by precinct &amp; other jurisdictional levels. Reports include: Zero, Grand Totals (long format), Precincts Processed, Totals by Precinct (long format) Machine Readiness, Audit log. Ensure audit logs are accurate &amp; complete and contain error and status messages.</li> <li>- Scan M650 ballots, then Scan Absentee ballots using separate media for each.</li> </ul> <p><b>Vote Consolidation into ERM:</b></p> <ul style="list-style-type: none"> <li>- <b>Discrepancy 20 (both scenarios):</b> verify no error "Convert Precinct Results File: The precincts results file is from older software and is being converted." And "Error: File: TC NAME.CTR, Error: #35 - File does not exist." "Is given when attempting to re-launch ERM.</li> <li>- <b>Discrepancy #9</b> - all 4 groups are displayed.</li> <li>- 3 ERM PCs will be used for reading results (DS200), and viewing and reading results simultaneously (M100 and M650)</li> <li>- Attempt to read in vote totals with test totals present. Verify message indicating there are totals present and a corrective action message is provided.</li> <li>- Admin account and password is needed in ERM System Administrator to prevent access to "Suspension Menu"; and confirm access is denied.</li> <li>- Geographic reports of votes; each contest by precinct &amp; other jurisdictional levels. Reports include: <ul style="list-style-type: none"> <li>- <b>Zero - RFI2008-07</b> to ensure ERM is zeroed out before processing election results.</li> <li>- <b>EL30A</b> - Prec Report–Group Detail individual precincts &amp; contest results.</li> <li>- <b>EL45</b> - Election Summary - total number of votes for each candidate/question &amp; % of total vote for each candidate/question</li> <li>- <b>EL111</b> - Name Heading Canvass - statistics of total number of precincts counted, total number of votes cast for each candidate and % of total vote received by each candidate</li> <li>- <b>EL50</b> - Precincts Counted - lists the identification numbers and names of your precincts the precincts that are counted by ERM.</li> <li>- <b>EL50A</b>, Precincts Completed Listing - list of precincts that have been completed along with their Total Ballots Cast, Total Registered Voters, and the Turnout Percentage</li> <li>- Audit log</li> </ul> </li> <li>- Consolidated reported votes match predicted votes from polling places, &amp; optionally other sources (absentee)</li> <li>- Retrieve ballot images from the DS200</li> <li>- Data from the M100, M650 &amp; DS200 is prevented from being altered or destroyed by report generation, or extraction from media</li> <li>- DS200 SN is displayed in ERM, once the USB flash drive is read into ERM</li> </ul>
Post-vote: Security	See Appendix C	<p>The central count: (See Security Test for detail)  During execution confirm:</p> <ul style="list-style-type: none"> <li>- Security access controls limit or detect access to critical systems&amp; the loss of system integrity, availability, confidentiality and accountability</li> <li>- Functions are only executable in the intended</li> </ul>

Method Detail	Reuse of SysTest System Level Test Method	Regression System Level Test Method
		<p>manner, order &amp; under the intended conditions</p> <p><b>Bug16348</b> Reporting of Overvotes</p> <ul style="list-style-type: none"> <li>- Prevented execution of functions if preconditions were not met</li> <li>- Implemented restrictions on controlled functions</li> <li>- Provided documentation of mandatory administrative procedures.</li> </ul> <p>COTS systems</p> <ul style="list-style-type: none"> <li>-Authentication is configured on the local terminal and external connection devices,</li> <li>-Operating systems are enabled for all session and connection openings, and closings, all process executions and terminations and for the alteration or detection of any memory or file object</li> <li>- Configure the system to only execute the intended and necessary processes during the execution of the election software. Election software process is halted until the termination of any critical system process, such as system audit.</li> </ul>
Post-vote: System Audit	See Appendix C	<p>The system audit provides a central count time stamped always available, report of normal and abnormal events that cannot be turned off when the system is in operating mode. Status message are part of the real time audit record.</p> <p>Audit Messages to be validated:</p> <p>VAT: date/time set DS200, M100 &amp; M650: Election id ERM: DS200 SN is recorded DS200, M100, M650 &amp; ERM: Message of vote totals present, Corrective action messages to resolve residual vote totals</p> <p>Status/Error messages to be validated:</p> <p>Re-use AIMS, AM, EDM, ESSIM, and HPM audit log results from ESSUNITY3200 (previously certified)</p> <p>VAT: System Maintenance (requires password), The Flash Card has been removed. Turn OFF the machine and insert a valid Flash Card. DS200 &amp; M100: Blank Ballot Rejected, More than one party has votes. Votes In Party Contests Will Be Ignored, Ballot Jammed, 119 – MULTIPLE BALLOTS DETECTED/Please Re-insert One Ballot After Beeps, One Contest Has Too Many Votes, Party Preference Race Missing</p>
Expected Results are observed	See Appendix C	<p>Review the test result against the expected result:</p> <ul style="list-style-type: none"> <li>• Accept: the expected result is observed</li> <li>• Reject: the expected result of the test case is not observed</li> <li>• Not Testable (NT): rejection of a previous test step prevents execution of this step, or tested in another TC.</li> <li>• Not Applicable (NA): not applicable to test scope</li> </ul>
Record observations and all input/outputs for each election;	<p>SysTest Unity 4.0.0.0 Test Plan identifies results validation:</p> <ul style="list-style-type: none"> <li>• Accept: expected results is observed</li> <li>• Reject: expected result is NOT observed</li> <li>• Not Testable (NT): rejection of a previous test step prevents validation of this step or this was tested in another test case</li> <li>• Not Applicable (NA): not applicable to the current test scope or to the component under review</li> </ul>	<p>All inputs, outputs, observations, deviations and any other information impacting the integrity of the test results will be recorded in the test case.</p> <ul style="list-style-type: none"> <li>- Any failure against the requirements of the EAC guidelines will mean the failure of the system and shall be reported as such.</li> <li>- Failures will be reported to the vendor as Defect Issues in the Discrepancy Report.</li> <li>- The vendor shall have the opportunity to cure all discrepancies prior to issuance of the Certification</li> </ul>

Method Detail	Reuse of SysTest System Level Test Method	Regression System Level Test Method
	<ul style="list-style-type: none"> <li>• Not Supported (NS): not supported in the current test scope</li> </ul>	<p>Report.</p> <p>- If cures are submitted the applicable test will be rerun. Complete information about the rerun test will be preserved in the test case. The cure and results of the retest will be noted in the Discrepancy Report and submitted as an appendix of the Certification Report.</p> <p>- Operations which do not fail the requirements but could be deemed defects or inconsistent with standard software practices or election practices will be logged as Informational Issues on the Discrepancy Report. It is the vendor's option to address these issues. Open items will be identified in the report.</p>

#### 7.4.1.3 DS200 Functional Test Result

iBeta conducted testing on the system configuration cross referenced in the test method below. Specific software and firmware builds for each test execution were recorded in the PCA Configuration as identified in the test case document.

Date	Test Result	Issues Opened	Issues Closed	Notes
3/3/2010	Accept			Scenario 3
3/19/2010	Accept			Rev. 1- Scenario 1
3/22/2010	Reject	#132		Rev. 1- Scenario 2: There is no Undervote query field in HPM.
3/25/2010	Accept			Rev. 1- Scenario 5
3/29/2010	Reject	#143		Rev. 1- Scenario 6: Counterfeit ballots were accepted.
3/30/2010	Accept		#132	Rev. 2- Scenario 2: Setting the Undervote query is done in EDM, not HPM.
4/6/2010	Accept			Rev. 2- Scenario 7
4/12/2010	Accept			Rev. 2- Scenario 4
4/12/2010	Accept		#143	Rev. 1- Scenario 6: The counterfeit ballot sensor functionality was withdrawn from Unity 3.2.1.0
9/17/2010	Reject	177 & 178		Modem Source Code Review Rev 00.
10/22/2010	Accept			Counterfeit Source Code Review Rev 00
11/12/2010	Accept		177	Modem Source Code Review Rev 01. Discrepancy 177 was added to a functional test Modem Check (Functional). 178 is documentation and remains open.
11/12/2010	Accept		177	Rev 00 Modem Check (Functional)
11/15/2010	Accept			Rev. 00 Scenario 10 Audit Log cast ballots, log on and log off
11/18/2010	Accept			Rev. 00 Scenario 11 Counterfeit Sensor
11/19/2010	Accept			Rev.00 Scenario 9 - 2 hour Back up Battery
12/13/2010	Not Tested			Scenario 8 – Not executed by 11/29/10; awaiting updated code
12/13/2010	Not Tested			Open discrepancy #178 not reviewed by 11/29/10, awaiting documentation

While documentation discrepancies may be encountered in testing they do not result in the rejection of a functional test. Identified issues are found in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#).

iBeta Definition	DS200 Functional Test Method
Test Case Name	DS200 Functional TC
Scope - identifies the type of test	<p>The scope is to test the DS200 Bug fixes and Enhancements:</p> <p>Functional testing for the following DS200 Bug fixes and Enhancements: ENH14725, ENH14726, ENH14729, ENH14730, ENH14731, ENH14732, ENH14745, ENH15009, ENH15287, ENH15288, ENH15418, BUG15827, ENH15890, ENH15891, ENH15892, ENH16085, ENH16120, ENH16211, ENH16231, ENH16382, ENH16291, ENH16336, ENG17266, ENH17268, ENH17538, BUG17666, ENH18150, ENH18555 ENH18562, ENH18681, ENH18807, BUG18687, ENH19168, ENH19169, ENH19170 19663, 19936</p> <p>Document Review of ES&amp;S BUG16775 &amp; BUG16782 for sufficiency of ES&amp;S testing.</p> <p>Source Code Review of the DS200 Freeze BUG18361, ENH18296, ENH18851 (ENH18851 is being tested functionally and through Source Code. See Scenario 8.)</p> <p>Source Code Review of the modem (no allowing external inputs) ENH14728</p> <p>Source Code Review of the disabling of Counterfeit Detection functionality ENH19323 &amp; Confirm functionally the change does not impact vote counting and reporting.</p> <p>ERM Enhancement BUG16384 for the state of IL</p> <p>System Halt Source Code Review (No Enhancement or Bug)</p>
Test Objective	<p>The objective for Scenarios 1-7 is to validate the ability to process, store and report data to the maximum and exceeding the maximum allowed number of precincts in a single polling place, BUGs and Enhancements to the DS200. To validate that the system generates errors during EMS ballot preparation (ballot preparation including: EDM, ESSIM &amp; HPM) when exceeding maximum the allowed number of precincts in a single polling place. Validating the processing, storing and reporting shall occur without system degradation. If there are system errors then the system shall recover without any loss of data.</p> <p>Test Objectives of Scenarios 8 &amp; 9 are associated with the DS200 freeze: S8) verify the error messages and audit logging associated with jams and halt S9) verify battery performance still meets the 2 hour minimum. Scenario 10 is to test and validate FRI 2009-04 and ENH19168, 19169 &amp; 19170</p>
Test Variables: Volume Stress Performance Error Recovery	<p><b>Scenario 1:</b> Create an Open Primary without Party Preference election:</p> <ul style="list-style-type: none"> <li>• <b>ENH16382-18 Precincts election day and 1 Polling Place</b> 9 District Types (this does not including Countywide) 18 District Name (two contests to ac district name) 18 ballot style (each precinct has its own ballot style) 14" 36 "standard 14" ballot 2 Partisan contest per style 4 candidates per contest (2 candidates/ party for the mayor contest, 4 candidates for the Senator contest (total of 216 candidates) Write-ins (1 for the Mayor and 2 for the Senatorial race) DEM and REP Parties</li> <li>• <b>ENH14745 &amp; BUG15827-the Scanner Options</b> Diverter is set for "Overvoted Write-ins &amp; Blank Ballots". Ballot Control is set to Query for "Overvoted ballots, Cross voted ballots, Unreadable marks, Undervoted ballots and blank ballots"</li> <li>• <b>ENH14725 •The DS200 scanner options are set to "Do not save any ballot images" ; Run Election set up reports in EDM</b></li> </ul> <p><b>Scenario 2: Same as Scenario 1 except:</b></p> <ul style="list-style-type: none"> <li>• <b>ENH15287 •Changes "election day" to "early voting" in HPM by selecting the "Include all Precincts" option. The early voting option allows the Poll worker to view ballot styles for that specific ballot box.</b></li> <li>• <b>ENH14725- The DS200 scanner options are set to "save all ballot images"</b></li> </ul> <p><b>Scenario 3: Same as Scenario 1 except:</b></p> <ul style="list-style-type: none"> <li>• <b>ENH16382 •19 precincts (exceeding new precinct limit)</b> <ul style="list-style-type: none"> <li>○ Add one extra District Name</li> <li>○ Add 2 contests (1 Mayor/1 Senator)</li> <li>○ Add 6 candidates for Party DEM (2 Mayor/4 Senator)</li> <li>○ Add 6 candidates for Party REP (2 Mayor/4 Senator) **If the EMS does not provide an error after exceeding the max precincts in a single polling place continue to DS200</li> </ul> </li> </ul> <p><b>Scenario 4: Same as Scenario 1 except:</b></p> <ul style="list-style-type: none"> <li>• <b>ENG15418 •ES&amp;S will provide ballots with speckling. Reuse the DS200 Functional S1 election.</b> Each ballot will contain stray marks in the time track (left hand side of the ballot). Marks will emulate various levels of white speckling. Ballot will be read on DS200 with v.</li> </ul>

iBeta Definition	DS200 Functional Test Method
	<p>1.3.10.0 and re-read on version 1.4.3.7</p> <ul style="list-style-type: none"> <li>• <b>ENH14726 &amp; ENH15288</b> After scanning a valid ballot, time how long the "Thank you for voting" screen displays. Note the time. Measure the font (text) on the "Thank you for voting" screen display. Note the size. Change firmware version and repeat test. Compare times and sizes.</li> </ul> <p><b>Scenario 5: Same as Scenario 1 except:</b></p> <ul style="list-style-type: none"> <li>• <b>ENH18150, ENH17538 &amp; 17666:</b> •Only testing the Protective Counter (for Maryland). Do not need the ballot box. ES&amp;S will provide an "updated" FW version that will have a different version number. To test, begin scanning ballots. Upgrade the firmware with the FW provided by ES&amp;S. Continue with voting. When the voting is complete, Verify the counter did not reset or lose count and the counter appears in the printed reports. Restore the DS200 to the original firmware version. Verify the counter did not lose count. <ul style="list-style-type: none"> <li>○ Note the counter number from the DS200 and the Initial State report; Load the election and scan a few (2 to 5) ballots; Close the polls</li> <li>○ NOTE The counter - from the results report and audit log; Upgrade the firmware; NOTE The counter on the Initial State report; Re-burn the media for the S1 election, load the election, and scan more ballots; Close the polls; Examine the protected counter on the DS200, Audit log and the Results report.</li> <li>○ Restore to the original firmware version; • Verify the protected counter did not lose count.</li> </ul> </li> </ul> <p><b>Scenario 6: Same as Scenario 1 except:</b></p> <p><b>ENH15009 &amp; 15891</b> (ES&amp;S has withdrawn support for DS200 counterfeit ballot detection from Unity 3210 on 4.09.10) <b>ENH19323</b> disables the functionality of ENH15009 and 15891.</p> <ul style="list-style-type: none"> <li>○ Calibrate the scanner and the counterfeit scanner using the steps in the "test data v1" tab.</li> <li>○ Scan counterfeit ballots (using vote tab under counterfeit ballots to vote)</li> </ul> <p><b>Scenario 7: Go to Regression REV01 TC Scenario 1 for testing of ENH16291/16336/EHN16120 Overvote translations.</b></p> <p><b>Scenario 8, 9, 10 &amp; 11 Reuse test election database and ballots</b></p>
A description of the voting system type and the operational environment	The Unity 3.2.1.0 EMS includes two types of configurations a Peer to Peer Network for Scenarios 1-6 and a 2003 Server based Network for Scenarios 7, 8 & 9  DS200 Precinct Count scanner Steel Ballot Box Plastic Ballot Box
VVSG 2005 vol. 1	2.1.5.1.b I thru vii, c, 2.1.6, 2.1.7.2, 2.2.1, 2.2.1.3, 2.3.1 thru 2.3.1.2, 2.1.4.j, 2.2.4, 2.3.3.1.b,c,d, 2.3.3.2, 2.4.1.b, 2.4.3, 2.4.2 thru 2.4.3, 4.1.5.1.d, 4.1.6.1, 4.1.8 thru 4.1.8  2.1.5.1, 2.1.5.1.b v & vi, 2.1.3 a & b, 2.1.4.g & i, 4.1.2.4.c
VVSG 2005 vol. 2	6.2, 6.2.1, 6.2.2, 6.3, 6.6, 6.7  A4.3.5 Volume (maximum and exceeding more than the maximum number of precincts in a Polling Place) A4.3.5 Volume/Stress (Processing, storing and reporting data when overloading the number of precincts in a Polling Place) A4.3.5 Performance/Recovery (Ballot format handling capability-graceful shut down and recovery without loss of data) A4.3.5 Performance/Recovery (Processing rates-graceful shut down and recovery without loss of data)
Hardware, Software voting system configuration and test place	<p>The Unity 3.2.1.0 <b>Peer to Peer</b> Voting System consists of the following: Audit Manger (AM ), Election Data Manger (EDM), ES&amp;S Ballot Image Manager (ESSIM), Hardware Program Manger (HPM), Model Election Reporting Manager (ERM), LogMonitor Service.</p> <p>1 @ Hub/switch, Peer to Peer Windows XP (Professional SP3 PC) file server 1 @ DS200 (1-DS200 version 1.3.10.0 and upgraded to @ version 1.4.3.x)</p> <p>The Unity 3.2.1.0 <b>2003 Server based Network</b> Voting System consists of the following: EMS Ballot Preparation SW: Audit Manager (AM), Election Data Manager (EDM), ES&amp;S Image Manager (ESSIM), Hardware Programming Manager (HPM), AutoMARK Information Management System (AIMS), Election Reporting Manager (ERM), LogMonitor Service Hardware: (5) Precinct Count scanner/tabulator: intElect DS200 (5 @ DS200 (all 5 with version 1.4.3.7) (1) File Server</p>

iBeta Definition	DS200 Functional Test Method
	<p>(2) PC for Unity and AIMS EMS applications          (2) PCs for ERM          (1) Network Printer          (1) Network hub/switch          5 @ DS200 (all 5 with version 1.4.3.7)          Test Location: iBeta, 2675 S. Abilene, Aurora, CO 80014</p>
Pre-requisites and preparation for execution of the test case.	<p>Complete the prerequisites:          Test Method Validation of the Import Wizard was completed in Volume 1</p> <ul style="list-style-type: none"> <li>- Excel spreadsheets saved as "Tab Delimited" with our baseline election data. Tab Delimited documents containing election creating information will be imported into EDM using the Import Wizard option.               <ul style="list-style-type: none"> <li>Spreadsheet 1 - Precincts 18</li> <li>Spreadsheet 2 - District Types 9</li> <li>Spreadsheet 3 - Districts Names 18</li> <li>Spreadsheet 4 - District Relations 18</li> <li>Spreadsheet 5 - Master Office 36</li> <li>Spreadsheet 6 - Office Relations 36</li> <li>Spreadsheet 7 - Candidates 144</li> </ul> </li> </ul> <p><b>Source Code review:</b> ENH18296, BUG18361 &amp; ENH18851 The Freeze Source Code Review has been completed without any issues prior to starting Scenario 8 &amp; 9</p>
Getting Started Checks	<p>Same as Volume 1 - Maximum Ballot Styles for paper on the M100;</p> <ul style="list-style-type: none"> <li>• <b>ENH17268, 15890, 15892 &amp; 17266</b> DS200 Functional TC environments include the updated scanner board firmware version, scanner client and FL implemented version.</li> <li>• <b>ENH19936 Discrepancy 186:</b> <ul style="list-style-type: none"> <li>• Verify a failure message appears and prints on the tape, firmware unsuccessfully installed</li> <li>• Verify after power on that the message appears again during start up.</li> </ul> </li> <li>• <b>ENH19663:</b> <ul style="list-style-type: none"> <li>• Verify "Modem Status: Not Detected"</li> <li>• Verify "Modem Status: Detected" in ES&amp;S test case</li> </ul> </li> </ul>
Documentation of Test Data & Test Results	Same as Volume 1 - Maximum Ballot Styles for paper on the M100;
Volume: Paper-based voting systems Processing	<p>Ballot Prep:</p> <ul style="list-style-type: none"> <li>-An election database can be accurately/securely defined &amp; formatted using the Import Wizard.</li> <li>-Ballots (candidates) can be accurately defined &amp; generated.</li> <li>• <b>Scenario 1)</b> Election can be created and installed with 18 Precincts in a single polling place poll place</li> <li>• <b>Scenario 2)</b> Same as scenario 1 except early voting and ballot images are saved</li> <li>• <b>Scenario 3)</b> Same as scenario 1 except over the maximum allowed number of Precincts in a single polling place poll place (19). Test execution of Scenario 3 is expected to stop at this point with errors generated in the ballot preparation prior to the creation of election media - Check audit logs for critical status messages. Test stops unless system does not error and creates media) - If EDM does not error during the "Ballot Sets Merge" then the EDM reports must be reviewed to verify 19 precincts have been created and assigned to a single polling place. Polling Place. Continue to ESSIM and HPM. The system should display a critical status message prior to exiting the HPM. - If there are any system errors that cause the EMS ballot preparation applications to crash then verify the applications recover without any loss of data. If no error is given prior to leaving HPM continue the test.</li> <li>• <b>Scenario 4)</b> Same as scenario 1 and ballots with stray marks are provided by ES&amp;S</li> <li>• <b>Scenario 5)</b> Same as scenario 1.</li> <li>• <b>Scenario 7)</b> Same as scenario 1 (Regression Test Case).</li> <li>• <b>Scenario 8, 9, 10 &amp; 11)</b> Same as scenario 1.</li> </ul>
Volume:	<p><b>Scenario 1 &amp; 3:</b> Overloading systems capacity to process, store, and report data.</p> <ul style="list-style-type: none"> <li>- When importing over the allowed amount of data into the EDM using the Import Wizard</li> <li>- Overloading the HPM with more than the allowed number of precincts in a single polling place.</li> </ul>
Stress	<b>Scenario 3:</b> System responses to overloading conditions. Exceeding the maximum allowed number of polling place precincts in a single Polling place.
Performance	<b>Scenario 1 &amp; 3:</b> There is no system degradation (Ballot format handling capability and Processing rates):

iBeta Definition	DS200 Functional Test Method
	<ul style="list-style-type: none"> <li>When importing large amount of data into the EDM using the Import Wizard.</li> <li>The system does not slow down throughout the testing</li> </ul> <p><b>Scenario 9</b> • DS200 can continue operation for 2 hours on battery backup</p>
Error Recovery	<p><b>Scenario 3, 8)</b> Same as Volume 1 - Maximum Ballot Styles for paper on the M100 except ENH18562: A graceful shut down occurs if the system errors "system halt" and powers down.</p> <p><b>Scenario 9)</b> If the system shuts down, the DS200 shuts down gracefully without loss or corruption of voting data previously stored.</p> <ul style="list-style-type: none"> <li>Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator.</li> <li>Resumption of normal operations (printing the audit log)</li> </ul> <p><b>System Halt Source Code Review:</b></p> <ul style="list-style-type: none"> <li>Search the code to identify each System Halt Event and Event Number</li> <li>Trace the halt; identify each instance of an error that generates the event and record the file, function, line and where the function is called</li> <li>Identify and record a description of the cause of the error</li> <li>Review the code and verify if both the event and the error/action generating the event are logged</li> </ul> <p><b>System Halt Document Review</b></p> <ul style="list-style-type: none"> <li>Review the documentation and confirm that each System Halt Event and Event Number is identified</li> </ul> <p><b>Disabling of Counterfeit Detection Document Review</b></p> <ul style="list-style-type: none"> <li>Review the documentation and confirm that each ES&amp;S has removed Counterfeit Detection functionality</li> </ul> <p><b>DS200 Modem Document Review</b></p> <ul style="list-style-type: none"> <li>Review the documentation and confirm that each ES&amp;S has removed modem functionality or the support of modem use.</li> </ul>
Readiness Testing and Poll Verification	<p><b>Scenario 1:</b> Voting system is ready for the election: Same as Volume 1 - Maximum ballot styles for paper</p> <ul style="list-style-type: none"> <li>Run 1 precinct to validate the system is ready; confirm the test data is segregated from voting data, with no residual effect. Verify totals and audit logs. <ul style="list-style-type: none"> <li><b>ENH14729</b> "Polls Opened Menu": Print the zero reports (first of 3 zero reports prior to opening of polls)</li> <li><b>ENH16231</b> a "Failure" error and a "Successful" message are displayed on the DS200, the audit log displays the Failure and Successful PW login attempts.</li> <li><b>ENH14729</b> The zero report can be printed. (second of 3 zero reports prior to opening the polls) The report continually displays zeros for the contest, candidates, precincts (all 18), under/overvotes and Write-Ins.</li> <li><b>ENH15287</b> The "Polls Opened Menu" doesn't display a "Ballot Style Report" button. (this displays only for Early Voting)</li> </ul> </li> <li><b>Scan pre-election test ballots,</b> <ul style="list-style-type: none"> <li><b>ENH14745</b> Select the options to override Overvoted ballots and Blank ballots only, do not select any other options. Overvoted and Blank ballots will not prompt an "Accept" or "Reject" message to the voter. The ballots will automatically be accepted due to the override. The Cross voted, Undervoted and unreadable ballots will provide a prompt to "Accept" or "Reject" and the voter will be required to make a selection</li> </ul> </li> <li>Tally pre-election test ballots; ballots match the predicted results outlined in the test case <ul style="list-style-type: none"> <li><b>ENH14732 &amp; ENH16211</b>•run the results tape; at the end of the Results tape and audit log they display the "Machine ID" and "Poll Number"</li> </ul> </li> </ul> <p><b>Scenario 2:</b></p> <ul style="list-style-type: none"> <li>Reuse the same election as Scenario 1 except with the changes noted in the Scenario 2 Voting Variations <ul style="list-style-type: none"> <li><b>ENH15287</b>• Verify the Ballot styles report button on the "Open Polls Menu" screen displays in the upper right hand of the icon bar and the report is accurate.</li> <li><b>ENH14745</b> Reset "Override" options: Selection the options to override (undervotes and crossover ballots) Verify ballots will automatically be accepted due to the override and "Overvoted W/I ballots", "Unreadable marks", and "Blank Ballots" will provide a prompt to "Accept" or "Reject" and the voter will be required to make a</li> </ul> </li> </ul>

iBeta Definition	DS200 Functional Test Method
	<ul style="list-style-type: none"> <li>selection</li> <li>○ <b>ENH14730</b> • Unplug the DS200 from the ballot box verify 2 beeps are heard. Print a zero report and open printer door while printing is occurring. Verify printing will stop and DS200 will beep two times.</li> <li>○ <b>ENH14730</b> 2 beeps and a "successful" message displays once the scanner has been calibrated (Calibrate scanner option).</li> <li>○ <b>ENH14730 (15890, 15892)</b>• Calibrate the counterfeit sensor; 2 beeps and a "successful" message displays (testing that only the counterfeit sensor can be set up as required, a message is displayed as well as 2 beeps can be heard once the counterfeit sensor has been successfully calibrated).</li> </ul> <p><b>Scenario 3:</b></p> <ul style="list-style-type: none"> <li>• Same as Scenario 1 except with the changes noted in the Scenario 3 Voting Variations</li> </ul> <p><b>Scenario 4:</b></p> <ul style="list-style-type: none"> <li>• Install Scenario 4 election database and run the zero report.</li> </ul> <p><b>Scenario 5:</b> Reuse the same election as Scenario 1</p> <ul style="list-style-type: none"> <li>• <b>ENH17538 &amp; 17666:</b> Note the counter number from the DS200 and the Initial State report.</li> </ul> <p><b>Scenario 8:</b></p> <ul style="list-style-type: none"> <li>▪ Set up DS200 with Queries</li> <li>▪ Enter incorrect and correct passwords (ENH18851: Initiate X-Windows calls utilizing the keyboard functions)</li> </ul> <p><b>Scenario 9:</b></p> <ul style="list-style-type: none"> <li>▪ Set up DS200 with Queries</li> </ul> <p><b>Scenario 10:</b></p> <ul style="list-style-type: none"> <li>▪ Test ballots, shut down, power up and check log for each ballot cast, all power downs and power ups.</li> </ul> <p><b>Scenario 11:</b></p> <ul style="list-style-type: none"> <li>• <b>ENH19323</b> Run checks from scenario 2 (ENH14730 (15891, 15890, 15892) is not observed) Counterfeit settings are disabled.</li> </ul> <p><b>Counterfeit Detection Source Code Review</b></p> <p><b>ENH19323</b> – Review the disabled Counterfeit Detection source code and verify: function "calibrate_cft_sensor_menu " is not being called in any other place within the code. No other code changes. Verify the following messages are not being called/used: 163 Counterfeit Calibration Menu Accessed, 164 Counterfeit Calibration Started, 165 Counterfeit Calibration Success, 166 Counterfeit Calibration Fail, 167 Counterfeit Multiplier Selected, 168 Counterfeit</p> <p><b>Modem Source Code Review</b></p> <p><b>ENH14728</b> – Review the modem source code and verify:</p> <ul style="list-style-type: none"> <li>• The code behavior is consistent and does not permit external inputs that can cause the system to enter an abnormal state</li> <li>• Attempts to modify code confirm <ul style="list-style-type: none"> <li>○ There is no ability to modify code or turn code on by inputs from the modem</li> <li>○ All data paths and memory locations used in vote recording protect against contamination of voting data (Checks and records)</li> <li>○ The audit record identifies that test data are expunged</li> </ul> </li> <li>• Code identifies the software/firmware version(s), the election, and the results of software and hardware diagnostic tests, including an entry if a modem or wireless transmission device is present and if present, its operable state</li> </ul> <p><b>Modem Document Review</b></p> <p><b>ENH14728</b> – Review the modem documentation in the TDP</p> <ul style="list-style-type: none"> <li>• The security procedures to ensure protection is maintained in the current status are developed and documented</li> <li>• The documentation contains the restriction that the presence of a log entry indicating a modem present nullifies the EAC certification of the DS200</li> </ul>
Pre- vote: Opening the Polls Verification	Precinct Count/ Paper based: Same as Volume 1 - Maximum Ballot Styles for paper on the M100; except no key position
Voting: Ballot Activation and Casting Verifications	<p><b>Scenario 1:</b> Using the predetermined vote pattern, mark and scan ballots.</p> <ul style="list-style-type: none"> <li>• <b>ENH16231</b> • attempt to reopen Polls using an incorrect and a correct password. Verify message appears on DS200 and in audit log.</li> </ul>

iBeta Definition	DS200 Functional Test Method
	<ul style="list-style-type: none"> <li>• <b>ENH14729</b> •Clear pre-election readiness test totals and run another zero report</li> <li>• <b>ENH14745</b> •Reset the "Override" options. Selecting the options to override Overvoted ballots and Blank ballots only, do not select any other options. Overvoted and Blank ballots will not prompt an "Accept" or "Reject" message to the voter. The ballots will automatically be accepted due to the override. The Cross voted, Undervoted and unreadable ballots will provide a prompt to "Accept" or "Reject" and the voter will be required to make a selection</li> <li>• <b>BUG15827</b>: Vote an Overvoted Write-in. Ballot is diverted into a separate bin on the steel ballot box.</li> <li>• <b>ENH14725 &amp; ENH16085</b> •View the icon bar for each of the icons on the "Welcome screen". Verify an X appears over the disk icon to indicate no images are being saved. Verify ballot status, power status, image status, election definition and open polls icons are displayed.</li> <li>• <b>ENH16382</b> •Vote ballots for all 18 precincts and verify the ballots for all 18 precincts are accepted without a precinct error</li> <li>• <b>ENH14731</b> •Verify that there is a beep as each ballot is accepted</li> <li>• <b>ENH14725</b> •The Welcome screen displays the Disk icon (on the icon bar) has a small red X (not saving ballot images)</li> <li>• <b>ENH16085</b> • Verify the Welcome screen displays the following on the icon bar, "Battery Status Indicator Icon, AC Power Status Indicator Icon, Image Saving Status Indicator Icon, Election Definition Status Icon"</li> </ul> <p><b>Scenario 2:</b></p> <ul style="list-style-type: none"> <li>• <b>ENH14725</b> •View the icon bar for each of the icons on the "Welcome screen". Verify no X appears over the disk icon to indicate images are being saved. All early voting ballots can be scanned without error into the correct ballot bin</li> </ul> <p><b>Scenario 3:</b></p> <ul style="list-style-type: none"> <li>• <b>ENH16382</b> •If the software accepts an election with 19 precincts, verify ballots for all 19 precincts can be scanned without error into the correct ballot bin</li> </ul> <p><b>Scenario 4:</b></p> <ul style="list-style-type: none"> <li>• <b>ENG15418</b> •ES&amp;S will provide ballots with speckling. Each ballot will contain stray marks in the time track (left hand side of the ballot). Marks will emulate various levels of white speckling. Ballot will be read on DS200 with v. 1.3.10.0 and re-read on version 1.4.3.7</li> <li>• Scan ballots <ul style="list-style-type: none"> <li>○ <b>ENH14726</b>: After scanning a valid ballot, time how long the screen displays "Thank you for voting". Note the time.</li> <li>○ <b>ENH15288</b>: After scanning a valid ballot, measure the font (text) on the "Thank you for voting" screen displays. Note the size.</li> </ul> </li> </ul> <p>Change the firmware version on the DS200</p> <ul style="list-style-type: none"> <li>• Scan ballots <ul style="list-style-type: none"> <li>○ <b>ENH14726</b>: After scanning a ballot, time how long the "Thank you for voting" screen displays. Note the time.</li> <li>○ <b>ENH15288</b>: After scanning a ballot, measure the font (text) on the "Thank you for voting" screen displays. Note the size.</li> </ul> </li> </ul> <p><b>Scenario 8 BUG18687</b> All candidates and Contest appear on the zero tape.</p> <ul style="list-style-type: none"> <li>• <b>ENH18555 &amp; 18807</b>: attempt to get error messages (191) displays on the DS200 screen: Ballot found in scanner during startup is ejected" is displayed on the DS200 screen</li> <li>• <b>ENH18681</b>: The DS200 does not hibernate.</li> </ul> <p><b>Scenario 9:</b> vote a total of 300 ballots will be voted in Precinct 1 (3 ballots a minute, 180 ballots an hour. <math>3 \times 120 = 360 - 60(20 \text{ minutes}) = 300</math> ballots for 1 hour and 40 minutes) 5 batches of 60 ballots. Each batch will take 20 minutes. Each ballot voted will have a query. The voter will accept each query.</p> <ul style="list-style-type: none"> <li>• <b>ENH18681</b>: The DS200 does not hibernate between batches.</li> </ul> <p><b>Scenario 10:</b></p> <ul style="list-style-type: none"> <li>• Scan ballots, shut down, power up</li> </ul>
Voting: Voting System Integrity, System Audit, Errors & Status Indicators	<p>Same as Volume 1 - Maximum Ballot Styles for paper on the M100; and</p> <p><b>Scenario 4:</b></p> <ul style="list-style-type: none"> <li>• <b>ENH15418</b> •Using a ballot with an estimated 10% of the timing track scratched out. Scan each ballot of the older DS200 version (v. 1.3.10.0) and on the new version. The old version will display an error the new version will allow the scanning of the ballot.</li> </ul>

iBeta Definition	DS200 Functional Test Method
	<ul style="list-style-type: none"> <li>• <b>ENH15418</b> •Using a ballot with an estimated 50% of the timing track scratched out. Scan each ballot of the older DS200 version (v. 1.3.10.0) and on the new version. The old version will display an error the new version will allow the scanning of the ballot.</li> <li>• <b>ENH15418</b> •The white marks (speckles) in the ballot time track will display error "BALLOT DRAGGED/Turn Ballot Over and Try Again" on version 1.3.10.0. (Cause: The ballot did not enter the feed mechanism smoothly, which caused misalignment during scanning.)</li> </ul> <p><b>Scenario 5:</b></p> <ul style="list-style-type: none"> <li>• <b>ENH17538 &amp; 17666:</b> <ul style="list-style-type: none"> <li>○ Scan a few (2 to 5) ballots. Close the polls. NOTE The counter - from the results report and audit log</li> <li>○ Upgrade the firmware. NOTE The counter on the Initial State report</li> <li>○ Re-burn the media for the S1 election, load the election, and scan more ballots. Close the polls</li> <li>○ Examine the protected counter on the DS200, Audit log and the Results report.</li> <li>○ Restore to the original firmware version.</li> <li>○ Verify the protected counter did not lose count.</li> </ul> </li> </ul> <p><b>Scenario 8:</b> examine the audit logs for messages 191 and 192 with a time and date stamp.</p> <p><b>Scenario 9:</b> Audit Log displays 300 Accepted Queries in Precinct 1, time and Date stamp &amp; all error messages. Date and time of normal and abnormal events is recorded. "error messages, query setting and accepting, battery events.</p> <p><b>ENH18681:</b> The DS200 does not hibernate.</p> <p><b>Scenario 10:</b></p> <ul style="list-style-type: none"> <li>▪ Verify log for each ballot cast, all power downs and power ups (including the test log ENH19168, 19169 &amp; 19170.</li> </ul> <p><b>Document Review of ES&amp;S Testing</b>  <b>BUG16775 &amp; BUG16782</b></p> <p>Review the ES&amp;S assessment, resolution and testing of the DS200 sporadically reporting a mark present in row 44 and row 45 of column D on the back of the ballot when no actual mark was present. Review the assessment of the issue on the DS200 FW (v.1.3.10.0) to confirm that it identified:</p> <ul style="list-style-type: none"> <li>• A very narrow set of specific variables required to generate the error.</li> <li>• ES&amp;S demonstrated they were able to consistently and reliably repeat the error; and</li> <li>• ES&amp;S' resolution was consistent with the VSS.</li> </ul> <p>Review the resolution testing to confirm that the testing included all conditions and was sufficient to accept without additional testing by iBeta.</p> <p><b>Variables Identified:</b> Location of the contest from the vertical timing tracks, proximity to the top or bottom of the ballot, left side of the column oval placement, extension of the text next to the oval the edge of the allowable print area specified in the print layout manuals, and insertion in a skewed fashion of ballots with no selection on the last contest in column D.</p> <p>Resolution: Tolerance adjustments such that ballots with these unique variables inserted in a skewed manner will be rejected and require reinsertion.</p>
Post-vote: Closing the Polls	<p><b>Scenario 1:</b> Once the polls are closed the voting system</p> <ul style="list-style-type: none"> <li>• Printed reports of ballots counted by tabulator</li> <li>• Reported votes match predicted votes from tabulator with votes and undervotes.</li> <li>• In the polling place print the summary report with all of the 18 precincts in a single polling place. <ul style="list-style-type: none"> <li>○ <b>ENH16211</b> •Cancel printing of audit log only and view the log displays for the "Machine ID" and "Poll Number". Print audit log; totals match the predicated reports (using the vote tab)</li> <li>○ <b>ENH16211</b> •Audit Log stops printing after cancellation and displays the "Machine ID" and "Poll Number" at the end of the Audit Log; •the Audit Log can be re-printed. The audit log will display the history of this election. The pretest and the Election Day audit log matches the pre-election activities outlined above.</li> <li>○ <b>BUG15827</b> •Overvoted Write-in ballots and blank ballots were separated from the other ballots</li> </ul> </li> </ul> <p><b>Scenario 2 and 4:</b> Same as Scenario 1 excluding the listed enhancements</p> <p><b>Scenario 3:</b> If the software accepts an election with 19 precincts, V the same as Scenario 1 excluding the listed enhancements</p>

iBeta Definition	DS200 Functional Test Method
	<b>Scenario 8, 9, 10:</b> Same are Scenario 1
Post-vote: Central Count	<p><b>Scenario 1:</b> ERM Zero report is printed and no totals display on the report prior to reading in the results. ERM: Vote Consolidation:</p> <ul style="list-style-type: none"> <li>• <b>ENH14725</b> • attempt to upload DS200 ballot images and a message displays stating no images saved. Ballot images from the DS200 CANNOT be extracted/ viewed. The image was not saved in HPM. (Ballot images not saved was set in Test Variables)</li> <li>• Votes match predicted votes (compare to vote tab. Vote tab is what was used to create paper ballots)</li> <li>• reports will display election identification</li> <li>• EL30A - Precinct Report–Group Detail, individual precincts &amp; contest results.</li> <li>• Precinct Report contains votes, undervotes &amp; overvotes</li> <li>• EL45- Election Summary, total number of votes for each candidate/question</li> <li>• Verify DS200 SN is displayed in ERM, once the USB flash drive is read into ERM</li> <li>• Ensure audit logs are accurate &amp; complete.</li> </ul> <p><b>Scenario 2:</b> Same as Scenario 1 except <b>ENH14725</b> • Upload DS200 ballot images. Ballot images from the DS200 can be extracted. The image was saved in HPM. (Ballot images saved was set in Test Variables)</p> <p><b>Scenario 3:</b> If the software accepts an election with 19 precincts, verify the same as Scenario 1 excluding the listed enhancements</p> <p><b>Scenario 4:</b> Do not import results into ERM because testing of EN15148 is restricted to the DS200.</p> <p><b>Scenario 8, 9, 10:</b> Same are Scenario 1 except only run the zero and Election Summary report.</p>
Expected Results are observed	Review the test result against the expected result: Same as Volume 1 - Maximum Ballot Styles for paper on the M100;
Record observations and all input/outputs for each election;	All inputs, outputs, observations, deviations and any other information impacting the integrity of the test results will be recorded in the test case. Same as Volume 1 - Maximum Ballot Styles for paper on the M100;

#### 7.4.1.4 DS200 Reliability Testing

Date	Test Result	Issues Opened	Issues Closed	Notes
11/11/2010	Test halted	187		<p>Discrepancy #187 recorded; test execution paused</p> <p>Until ES&amp;S provides a root cause analysis that can substantiate if the system diverted from the intended path that increments the counter it cannot be determined if discrepancy #187 is a failure of the Reliability Test Case. A new code delivery will require a complete re-test.</p>

iBeta Definition	DS200 Reliability Test Method
Test Case Name	DS200 Reliability Test Case (Field Issue - Freeze)
Scope - identifies the type of test	<p>Examine ESS' diagnostic testing of the DS200 random freeze to identify a baseline incidence of freeze failures.</p> <p>Run the test script on the ESSUnity3200 certified DS200 to establish if there is consistency of results with the ESS testing and calculate the system availability for the system configuration identified in the ESS DS200 predicted model.</p> <p>Conduct a reliability test to confirm the Mean Time Between Failure (MTBF) shall be at least 163 hours. Calculate if availability is 99% or greater using the in the ESS DS200 predicted model .</p>
Test Objective	Demonstrate that the DS200 shall operate at least 163 hours without loss of one or more functions or degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds.
Test Variables:	<p>Comparison for Consistency of Results:</p> <p>5 @ DS200 FW v.1.3.10.1</p> <p>Regression Test Case election database</p> <p>Execute ESS Touch Test scripts until one of the following is reached:</p> <ul style="list-style-type: none"> <li>• 100 tests (20 per DS200); or</li> </ul>

iBeta Definition	DS200 Reliability Test Method
	<ul style="list-style-type: none"> <li>• 10 combined failures (prior to execution of 100 test elections)</li> </ul> <p>Consistency of Results is established:</p> <ul style="list-style-type: none"> <li>• Observation of an 8 to 13% overall failure rate</li> </ul> <p>Reliability Test :</p> <p>3 @ DS200 FW 1.4.3.7 with the highest incidence of failure in the Comparison</p> <p>Power cycling variables:</p> <ul style="list-style-type: none"> <li>• 1@ DS200 restarted after each test;</li> <li>• 1@ DS200 restarted at the end of each day; and</li> <li>• 1@ DS200 remains for the full 64 hours.</li> </ul> <p>DS200 v.1.4.3.7 calls to the X Windows library include:</p> <ul style="list-style-type: none"> <li>• Source/GUI/src/KeySim.cpp (generates X events to simulate keyboard button presses) - ESS script - entry of password on the keyboard</li> <li>• Source/HAL/PmtlInfo.cpp (generates keyboard events sent to X server, convert X-server char values and printable char values) ESS script - entry of password on the keyboard and printing reports</li> <li>• Source/TouchScreen/src/cal.c (create calibration window &amp; Recalibrate &amp; Exit buttons) - Augmented script - add screen calibration steps to the election</li> <li>• Source/TouchScreen/src/xf86Elo.c (modified - functions for X server to load/unload driver) - Pre-requisite - Installation of v.1.4.3.7</li> </ul> <p>Regression Test Case election database</p> <p>Execute 120 (3 x 40) Touch Test scripts; then</p> <p>Execute for the remaining time test elections incorporating the Augmented Script. Additions to the Touch Test script included:</p> <ul style="list-style-type: none"> <li>• Administrator screen calibration;</li> <li>• Opening the polls and running a zero count report;</li> <li>• 8 voting sessions with voter query screen touches (2 ballots @ querying for an undervotes, overvotes, blank ballots or crossover vote); and</li> <li>• Closing the polls and printing reports</li> </ul> <p>Each machine will complete 64 hours (8 days X 8 hr)</p> <p>Acceptance Criteria:</p> <ul style="list-style-type: none"> <li>• No loss of any function (freeze or auto shut down) ; and</li> <li>• No degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds. If a unit recovers and performs its intended function without operator intervention in less than 10 seconds it shall not be identified as a failure. If a potential freeze is identified the tester shall wait 10 seconds after the expect interval for normal operation. The tester shall then confirm if the unit is frozen.</li> </ul> <p>Availability is <math>99\% = OR &gt; MTBF/(MTBF + MTTR)</math> for the configuration identified in the DS200 predicted model.</p>
A description of the voting system type and the operational environment	<p>Comparison:</p> <p>ESSUnity3200 EAC Certified DS200 precinct optical scanner with FW v.1.3.10.1</p> <p>Reliability&amp; Availability:</p> <p>Unity 3.2.1.0 DS200 precinct optical scanner with FW v.1.4.3.7</p>
VVSG 2005 vol.1	2.1.1b, 2.1.3, 2.1.4.g, 2.1.4.i, 2.1.5.1, 4.3.3, 4.3.5
VVSG 2005 vol.2	4.7.3, 4.7.4
Hardware, Software voting system configuration and test location	<p>Comparison:</p> <p>5 @ DS200 SN &amp; HW versions are identified in Table 12</p> <p>DS200 FW v.1.3.10.0</p> <p>Regression:</p> <p>3 @ DS200 precinct optical scanner with highest incidence of failure in the Comparison</p> <p>DS200 FW v.1.4.3.7.</p>
Pre-requisites and preparation for execution of the test case.	<p>Comparison Reliability: On each DS200 run the ESS Touch Test script 20 times. Record each step as completed.</p> <ul style="list-style-type: none"> <li>• Insert the USB with the election; press the "Power" button; the DS200 will take approximately two minutes to boot. <ul style="list-style-type: none"> <li>◦ Verify "Election Definition Found"</li> </ul> </li> </ul>

iBeta Definition	DS200 Reliability Test Method
	<ul style="list-style-type: none"> <li>• Access the Administrative Mode - Date &amp; Time             <ul style="list-style-type: none"> <li>◦ Select the Arrow (bottom right side of the touchscreen); select "Go To Admin" button; enter the correct password; select Enter;</li> <li>◦ Screen displays "Administration Mode; select "System Settings"; select "Date &amp; Time" ;</li> <li>◦ Scroll from the top of the Time Zones to the Bottom of all available time zones; return to EST time zone which was previously set; and</li> <li>◦ Exit Date &amp; Time, System Settings &amp; Admin Menu.</li> </ul> </li> <li>• Change the password; repeat these steps 20 times:             <ul style="list-style-type: none"> <li>◦ Select the Arrow (bottom right side of the touchscreen); select "Go to Admin" button; enter the correct password; select Enter; and Exit Admin Menu.</li> </ul> </li> <li>• Power off; remove the memory stick and archive the PCB file; confirm all test steps are completely recorded in the test record.</li> </ul> <p>Comparison Availability calculation:      Record all operating time. If a failure occurs, record the type and assign the appropriate MTTR.      At the end of testing total all operating time to identify the MTBF and all MTTR. Calculate:  <math>\text{Availability} = \text{MTBF}/(\text{MTBF} + \text{MTTR})</math></p> <ul style="list-style-type: none"> <li>• 2 hours = Hardware Failure and Major Ballot Jam MTTR</li> <li>• .25 hours =Freeze/restart or minor ballot jam MTTR</li> </ul>
Getting Started Checks	<p>Getting Started: Complete the prerequisites      Check the voting system to:</p> <ul style="list-style-type: none"> <li>• Verify the test environment and system configuration is documented in the PCA Configuration .</li> <li>• Validate installation of the trusted build</li> <li>• Testers understand that no change shall occur to the test environment without documentation in the test record and the authorization of the project manager.</li> <li>• During testing an operational readiness test was performed.</li> </ul> <p>Ballots match the election database</p>
Documentation of Test Data & Test Results	<p>Test Data: Record all programmed &amp; observed election, ballot &amp; vote data fields and field contents on the corresponding tabs of the test case in order to provide a method to repeat the test      Preserve all tabs for each instance the test is run.</p> <p>Comparison for consistency:</p> <ul style="list-style-type: none"> <li>• Record the start and stop time of each ESS Touch Test script. If the test script is completed, record the test as "Complete". If the stop is due to a freeze record test as "Freeze". If the stop is due to another condition record "Other" and provide full details.</li> <li>• Record the time of freezes.</li> <li>• Record the availability failures record type and the appropriate MTTR from the ESS Predicted Model; restore the DS200 to system to operation after a jam, failure or freeze.</li> <li>• Record any error message and time.</li> <li>• On the tape, note the machine ID and record the test execution number and tester; save the data files to the test recording PC. Label the folder with the machine ID and test execution number, for delivery to the EAC.</li> </ul> <p>Reliability:</p> <p>If in 64 hours on 3 @ DS200 there is a loss of one or more functions or degradation of performance greater than 10 seconds record the test as Reject. If there is no loss of function or degradation mark it Accept.</p> <ul style="list-style-type: none"> <li>• In Comments enter any deviations, discrepancies, or notable observations</li> <li>• Log discrepancies on the Discrepancy Report and insert the discrepancy number in the Comments field of Test Step.</li> </ul> <p>For the first 120 (3 X 40) ESS Touch Test script:</p> <ul style="list-style-type: none"> <li>• Follow the instructions listed in the Comparison</li> </ul> <p>For the Augmented script:</p> <ul style="list-style-type: none"> <li>• Record each test execution and the ballot counter. If a unit is stopped due to a freeze or other failure record the ballot processed, any ballots in the DS200 or transport and halt testing. If the unit is stopped due to a jam, continue testing.             <ul style="list-style-type: none"> <li>◦ Record the time of jams and the number of ballots processed.</li> <li>◦ Record the jam type and MTTR, restore the DS200 to system to operation.</li> </ul> </li> </ul>

iBeta Definition	DS200 Reliability Test Method
	<p>Identify the disposition of any ballot in the DS200 or transport.</p> <ul style="list-style-type: none"> <li>Record any error message and time.</li> </ul> <p>On the tape, note the machine ID and record the test execution number and tester; save the data files to the test recording PC. Label the folder with the machine ID and test execution number, for delivery to the EAC</p>
Reliability	<p>3 @ DS200 with the highest incidence of failure in the Comparison</p> <p>For the first 120 iterations (3 x 40) use the ESS Touch Test script. On the 41st use the Augmented Touch Test script incorporating the DS200 functionality that uses X-Windows calls.</p> <ul style="list-style-type: none"> <li>Repeat the test script on each DS200 for 64 hours (8 days X 8 hours) or until any one DS200 experiences: <ul style="list-style-type: none"> <li>A loss of any function; and</li> <li>Degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds</li> </ul> </li> <li>Record each iteration of testing, confirm all test steps are completely recorded in the test record, and archive the PCB file.</li> </ul>
Availability	<p>Availability: Record all operating time. If ballot jam occurs, record the type and assign the appropriate MTTR. At the end of testing total all operating time to identify the MTBF and all MTTR.</p> <p>Calculate: Availability =MTBF/(MTBF +MTTR).</p> <ul style="list-style-type: none"> <li>2 hours = Major Ballot Jam MTTR</li> <li>.25 hours =Minor ballot Jam MTTR</li> </ul>
Expected Results are observed	<p>Review the test result against the expected result:</p> <ul style="list-style-type: none"> <li>Accept: the expected result is observed</li> <li>Reject: the expected result of the test case is not observed</li> <li>Not Testable (NT): rejection of a previous test step prevents execution of this step, or tested in another TC.</li> <li>Not Applicable (NA): not applicable to test scope</li> </ul>
Record observations and all input/outputs for each election;	<p>All inputs, outputs, observations, deviations and any other information impacting the integrity of the test results will be recorded in the test case.</p> <ul style="list-style-type: none"> <li>Any failure against the requirements of the EAC guidelines will mean the failure of the system. and shall be reported as such.</li> <li>Failures will be reported to the vendor as Defect Issues in the Discrepancy Report.</li> <li>The vendor shall have the opportunity to cure all discrepancies prior to issuance of the Certification Report</li> <li>If cures are submitted the applicable test will be rerun. Complete information about the rerun test will be preserved in the test case. The cure and results of the retest will be noted in the Discrepancy Report and submitted as an appendix of the Certification Report</li> <li>Operations which do not fail the requirements but could be deemed defects or inconsistent with standard software practices or election practices will be logged as Informational Issues on the Discrepancy Report. It is the vendor's option to address these issues. Open items will be identified in the report.</li> </ul>

#### 7.4.2 FCA Volume (Volume Stress, Performance and Error Recovery) Testing

iBeta conducted the Volume tests on the system configuration identified in the PCA Configuration and the individual test methods below. Specific software and firmware builds for each test execution are recorded in the PCA Configuration as identified in the individual test case document.

##### 7.4.2.1 Volume 1 Test Results

Date	Test Result	Issues Opened	Issues Closed	Notes
9/22/2009	Accept			Scenario 1

No functional issues were identified. While documentation discrepancies may be encountered in testing they do not result in the rejection of a functional test.

Method Detail	Volume 1 Test Method
Test Case Name	Volume 1 - Maximum Ballot Styles for paper on the M100
Scope - identifies the	The scope of this test 1639 precincts,1639 ballot styles reusing the unmodified election data created

Method Detail	Volume 1 Test Method
type of test	<p>in <b>ESSUNITY3200</b>: The election data was created on a stand alone PC configuration however, the election will be loaded on a -to-peer configuration (multiple PCs) set up.</p> <p><b>Scenario 1)</b> The maximum number of ballot styles allowed for paper based systems (M100).</p>
Test Objective	<p>The objective is to validate the ability of the M100 to process, store and report data using the allowed maximum number ballot styles with 1639 precincts within an election using a peer-to-peer configuration. iBeta will reuse the results from <b>ESSUNITY3200</b> for exceeding the maximum numbers of ballot styles (HPM limitation and not a hardware limitation). The test is only to validate the processing, storing and reporting without system degradation. If there are system errors that cause the system to crash the system shall recover without any loss of data.</p>
Test Variables: Volume Stress Performance Error Recovery	<p>Reuse the Volume 1 Election database from the <b>ESSUNITY3200</b> test effort and verify the election contains the following:</p> <p>General Election, Election Day (M100)  Partisan, Vote for 1  4 Ovals per Inch ballot - (14" ballot, 48 ovals positions per Column, 6 columns, 288 total positions)  4 candidates per contest</p> <p><b>Scenario 1)</b> 1639 precincts with 1639 ballot styles (Maximum precincts/Maximum ballot styles)</p> <ul style="list-style-type: none"> <li>- Contests 1 - 290 in Polling Places 1 -29 (10 precincts to a polling place, 3 contest to a precinct) total of 290 ballot styles</li> <li>- No contest/Precincts assigned to Polling Places 30 -290</li> <li>- Contests 291 - 1639 in Polling Places 291- 1639 (1 precinct to a polling Place, 3 contest to a polling place) 1348 ballot styles</li> <li>- Contest 1639 in Polling Place 1639 with Precincts 1639 (3 contest in the precinct, and all polling places) 1 ballot style</li> </ul> <p>-The election can be loaded on the M100 media.</p>
A description of the voting system type and the operational environment	<p>The Unity 3.2.1.0 EMS includes a peer-to-peer Network:</p> <p>Reusing the ES&amp;S <b>ESSUNITY3200</b> Volume 1 election database to validate the maximum limitation of 1639 ballot styles for paper (M100 Precinct Count scanner) and using a peer-to-peer PC configuration in the EMS.</p>
VSS 2002 vol. 1	<p>2.2.5.2.2 Audit/Error messages  2.2.5.2.3 Audit/Status messages  2.2.3 Error Recovery</p>
VSS 2002 vol. 2	<p>6.2.3 Volume (maximum number of ballot styles)  A4.3.5 Volume (maximum number of ballot styles)  A4.3.5 Volume/Stress (Processing, storing and reporting data when overloading the number of precincts in a Polling Place)  A4.3.5 Performance/Recovery (Ballot format handling capability-graceful shut down and recovery without loss of data)  A4.3.5 Performance/Recovery (Processing rates-graceful shut down and recovery without loss of data)</p>
Hardware, Software voting system configuration and test location	<p>The Unity 3.2.1.0 Voting System consists of the following:</p> <p>Audit Manager (AM), Election Data Manager (EDM), ES&amp;S Ballot Image Manager (ESSIM), Hardware Program Manager (HPM), Model 100 (M100), Election Reporting Manager (ERM), AutoMARK Information (AIMS), Voter Terminal (VAT), LogMonitor</p> <p>1 @ marking device: Voter Terminal (VAT)  1 @ Unity 3.2.1.0 precinct count includes: M100  1 @ Unity 3.2.1.0 central count tally: Election Reporting Manager (ERM)  1 @ Hub/switch, peer-to-peer Windows XP (Professional SP3 PC) file server</p> <p>All testing is performed by iBeta LLC located at 3131 S. Vaughn Way, Aurora, CO 80014.</p>
Pre-requisites and preparation for test case execution	<p>Complete the prerequisites:</p> <p>Test Method Validation: Reuse of Technical review conducted by C. Coggins; Approved 3/4/09 for validation of test method as defined in ISO/IEC 17025 clause 5.4.5; acceptance of the test method by EAC documented with issuance of EAC certification number <b>ESSUnity3200</b>.</p> <p>Successful use of the Import Wizard to import large amounts of data into EDM tested and validated: 3/18/09 in <b>ESSUNITY3200</b></p> <p>Reuse of the Election data created by the Import Wizard must be on the peer-to-peer Windows XP</p>

Method Detail	Volume 1 Test Method
	(Professional SP3) PC.
Getting Started Checks	<p><b>Getting Started:</b> Complete the prerequisites;  Check the voting system to:  <ul style="list-style-type: none"> <li>- Verify the test environment and system configuration is documented in the PCA Configuration and vendor described configuration.</li> <li>- Validate installation of the unmodified <b>ESSUNITY3200</b> SW/FW and Unity 3.2.1.0 trusted build</li> <li>- Testers understand that no change shall occur to the test environment without documentation in the test record and the authorization of the project manager.</li> <li>- During testing an operational readiness test was performed.</li> <li>- The environment is set up with a peer-to-peer configuration: 1 PC for Unity ballot preparation SW, 1 PC for AIMS, 1 PC for ERM</li> </ul> </p>
Documentation of Test Data & Test Results	<p>Test Data:</p> <ul style="list-style-type: none"> <li>- Record all programmed &amp; observed election, ballot &amp; vote data fields and field contents on the corresponding tabs to provide a method to repeat the test</li> <li>- Preserve all tabs for each instance the test is run.</li> </ul> <p>Test Results:</p> <ul style="list-style-type: none"> <li>- Enter Accept/Reject on the Test Steps</li> <li>- In Comments enter any deviations, discrepancies, or notable observations</li> <li>- Log discrepancies on the Discrepancy Report and insert the discrepancy number in the Comments field of Test Step.</li> </ul>
Volume: Paper-based voting systems Processing	<p>Reuse the Volume 1 Election database from the <b>ESSUNITY3200</b> test effort and verify the election contains the following:</p> <ul style="list-style-type: none"> <li>- 4 candidates per contest</li> <li>- 1639 Ballot Styles</li> <li>- 1639 Precincts</li> <li>- 1639 Polling Places</li> </ul> <p>An election database was accurately/securely defined &amp; formatted using the Import Wizard.</p> <ul style="list-style-type: none"> <li>- Set up election by Style</li> <li>- Ballots (candidates &amp; propositions) were accurately defined &amp; generated.</li> <li>- Check EDM reports for election set up</li> <li>- Election media was installed</li> <li>- There were no system errors that caused the EMS ballot preparation applications to crash.</li> </ul>
Volume:	<p>System response to processing more than the expected number of ballot styles in an election. Maximum capacity is successfully processed without errors.</p> <p>Overloading system's capacity to process, store, and report data.</p>
Stress	<p>System responses to overloading conditions is generating an error in the EMS, it is not applicable to testing on the M100.</p> <p>Reuse results from <b>ESSUNITY3200</b> Test report Appendix D, section 7.4.2 Volume 1 Scenario 2</p>
Performance	<p>No system degradation (Ballot format handling capability and Processing rates) is observed:</p> <ul style="list-style-type: none"> <li>- When installing an election with 1639 precincts and ballot styles onto each device (M100)</li> <li>- The system will not slow down as more and more data is added</li> </ul>
Error Recovery	<p>Voting system gracefully shuts down (no crash) and recovers from errors caused by overloading the number of precincts and ballots styles.</p> <ul style="list-style-type: none"> <li>- Ballot format handling capabilities and processing capabilities-graceful shut down and recover without loss of data</li> <li>- Critical Status Messages</li> </ul>
Readiness Testing and Poll Verification	<p>Verify the voting system is ready for the election:</p> <ul style="list-style-type: none"> <li>- The election is correctly installed (Election ID, polling place name, precincts)</li> <li>- Test data (run 2 different precincts to validate the system is ready) is segregated from voting data, with no residual effect'</li> </ul> <p>Test confirmation that there are:</p> <ul style="list-style-type: none"> <li>- No hardware/software failures</li> <li>- The device is ready to be activated to accept votes (No Identification of any failures &amp; corrective action)</li> </ul>
Pre- vote: Opening the Polls Verification	<p>Verify the polling place voting system:</p> <ul style="list-style-type: none"> <li>- Zero count report has no results. All test results have been zeroed out during readiness testing.</li> <li>- Election identification including, Election Name/ID, Precinct ID/Name, Firmware Version</li> <li>- Key is turned to the Vote position and a message is displayed "Insert ballot"</li> </ul>
Voting:	Protects secrecy of ballot/vote

Method Detail	Volume 1 Test Method
Ballot Activation and Casting Verifications	<ul style="list-style-type: none"> <li>- Reuse the ballots marked by the VAT during the <b>ESSUNITY32000</b> certification effort.</li> <li>- Scan the ballots using the M100 (Election Day)</li> <li>- Vote a sample of the 1639 precincts (approximately 10%).</li> <li>- Vote 21 precincts each with a different ballot style</li> <li>- Each precinct will contain 3 contests with 4 candidates</li> <li>- Records selections and non-selection of individual choices for each contest</li> <li>- Increment the ballot counter</li> </ul>
Voting: Voting System Integrity, System Audit, Errors & Status Indicators	<p>The system audit provides a time stamped, always available, report of normal/abnormal events found within the percentage of sampled test (approximately 10%).</p> <p><b>Error messages are:</b></p> <ul style="list-style-type: none"> <li>- Generated, stored and reported as they occur</li> <li>- Errors requiring intervention by the voter or poll worker are clearly displayed issues and action instructions in easily understood non-technical text language or with indicators</li> <li>- The text for any numeric codes is contained in the error or affixed to the inside of the voting system</li> <li>- Incorrect responses will not lead to irreversible errors.</li> <li>- Nested conditions are corrected in the sequence to restore the system to the state before the error occurred</li> </ul> <p><b>Status Messages are:</b></p> <ul style="list-style-type: none"> <li>- Displays and reports critical status messages using unambiguous indicators or English language text.</li> <li>- Non-critical status messages are displayed but does not have to be at the time of occurrence and may be numerical codes for subsequent interpretation and reported in unambiguous text.</li> <li>- Status messages are part of the real-time audit record.</li> </ul>
Post-vote: Closing the Polls	<p>Once the polls were closed the voting system</p> <ul style="list-style-type: none"> <li>- Printed reports of ballots counted by tabulator</li> <li>- Reported that votes match predicted votes from the tabulator with votes and undervotes.</li> <li>- Records selections and non-selection of individual choices for each contest</li> </ul>
Expected Results are observed	<p>Review the test result against the expected result:</p> <ul style="list-style-type: none"> <li>• Accept: the expected result is observed</li> <li>• Reject: the expected result of the test case is not observed</li> <li>• Not Testable (NT): rejection of a previous test step prevents execution of this step, or tested in another TC.</li> <li>• Not Applicable (NA): not applicable to test scope</li> </ul>
Record observations and all input/outputs for each election;	<p>All inputs, outputs, observations, deviations and any other information impacting the integrity of the test results will be recorded in the test case.</p> <ul style="list-style-type: none"> <li>- Any failure against the requirements of the EAC guidelines will mean the failure of the system. and shall be reported as such.</li> <li>- Failures will be reported to the vendor as Defect Issues in the Discrepancy Report.</li> <li>- The vendor shall have the opportunity to cure all discrepancies prior to issuance of the Certification Report.</li> <li>- If cures are submitted the applicable test will be rerun. Complete information about the rerun test will be preserved in the test case. The cure and results of the retest will be noted in the - Discrepancy Report and submitted as an appendix of the Certification Report.</li> <li>- Operations which do not fail the requirements but could be deemed defects or inconsistent with standard software practices or election practices will be logged as Informational Issues on the Discrepancy Report. It is the vendor's option to address these issues. Open items will be identified in the report.</li> </ul>

#### 7.4.2.2 Volume 2 Test Results

Date	Test Result	Issues Opened	Issues Closed	Notes
9/24/2009	Accept			Scenario 1 & 2

No functional issues were identified. While documentation discrepancies may be encountered in testing they do not result in the rejection of a functional test.

Method Detail	Volume 2 Test Method
Test Case Name	Volume 2 - Maximum Ballot Styles in a Single Precinct on the M100
Scope - identifies the type of test	<p>The scope is to test the maximum numbers of ballot styles on the M100 in a single precinct.</p> <p><b>Scenario 1)</b> The maximum allowed number of 40 ballot styles on the M100 within a single precinct.</p>

Method Detail	Volume 2 Test Method
	To verify that errors are generated in scenario 2: <b>Scenario 2)</b> Exceeding the maximum allowed number of 40 ballot styles on the M100 within a single precinct.
Test Objective	The objective is to validate the ability to process, store and report data when using the allowed maximum number of ballot styles within a single precinct in a peer-to-peer configuration. To validate that the system generates errors during EMS ballot preparation (ballot preparation will only include the HPM since the election database was created in <b>ESSUNITY3200</b> and being reused) when exceeding the maximum numbers of ballot styles within a single precinct. Validating the processing, storing and reporting shall occur without system degradation. If there are system errors that cause the system to crash the system shall recover without any loss of data.
Test Variables:	Reuse the Volume 1 Election database from the <b>ESSUNITY3200</b> test effort and verify the election contains the following: General election for each scenario 1 Precinct with 40 splits Vote for 1 & Vote for N of M Oval Positions Left Certified Write-Ins 5 contest for each ballot style 4 candidates for each contest  Election day (M100) 40 Ballot Styles on the M100 Maximum ballot styles Election set up for the M100 (Reuse election files from <b>ESSUNITY3200</b> Vol. 2) Non-partisan offices one page ballot 4 Ovals per Inch ballot - (19 inch ballot, 68 ovals positions per Column, 6 columns per ballot, 408 total oval positions) Election Day Voting (M100) <b>Scenario 1)</b> 1 precinct with 40 Ballot Styles on the M100 <b>Scenario 2)</b> 1 precinct with 41 Ballot Styles on the M100
A description of the voting system type and the operational environment	The Unity 3.2.1.0 EMS includes a peer-to-peer Network: Reusing the ES&S <b>ESSUNITY3200</b> Volume 2 election database to validate the maximum limitation of 40 ballot styles for paper (M100 Precinct Count scanner) and using a peer-to-peer PC configuration.
VSS 2002 vol. 1	• Same as Volume 1 - Maximum Ballot Styles for paper on the M100
VSS 2002 vol. 2	• Same as Volume 1 - Maximum Ballot Styles for paper on the M100
Hardware, Software voting system configuration and test location	• Same as Volume 1 - Maximum Ballot Styles for paper on the M100
Pre-requisites and preparation for test case execution	• Same as Volume 1 - Maximum Ballot Styles for paper on the M100
Getting Started Checks	<b>Getting Started:</b> Complete the prerequisites; Check the voting system to: - Verify the test environment and system configuration is documented in the PCA Configuration and vendor described configuration. - Validate installation of the witnessed build - Testers understand that no change shall occur to the test environment without documentation in the test record and the authorization of the project manager. - During testing an operational readiness test was performed. - The environment is set up with a peer-to-peer configuration. (Configuration is as follows: 1 PC for Unity ballot prep. software, 1 PC for AIMS, 1 PC for ERM)
Documentation of Test Data & Test Results	Test Data: - Record all programmed & observed election, ballot & vote data fields and field contents on the corresponding tabs to provide a method to repeat the test - Preserve all tabs for each instance the test is run. Test Results: - Enter Accept/Reject on the Test Steps

<b>Method Detail</b>	<b>Volume 2 Test Method</b>
	<ul style="list-style-type: none"> <li>- In Comments enter any deviations, discrepancies, or notable observations</li> <li>- Log discrepancies on the Discrepancy Report and insert the discrepancy number in the Comments field of Test Step.</li> </ul>
Volume: Paper-based voting systems Processing	<p>Reuse the Volume 1 Election database from the <b>ESSUNITY3200</b> test effort and verify the election contains the following:</p> <p><b>Scenario 1</b> maximum limits:</p> <ul style="list-style-type: none"> <li>1 Precinct</li> <li>Vote for 1 &amp; Vote for N of M 19 inch ballot</li> <li>5 contest for each ballot style</li> <li>4 candidates for each contest</li> </ul> <ul style="list-style-type: none"> <li>-Election day (M100)</li> <li>- 40 Ballot Styles on the M100 (M100 Maximum ballot styles) allowed in a single precinct</li> <li>- Election set up for the M100</li> <li>- If there are any system errors that cause the EMS ballot preparation applications to crash then verify the applications recover without any loss of data.</li> </ul> <p><b>Scenario 2</b> Exceeding limits:</p> <ul style="list-style-type: none"> <li>- 41 Ballot Styles on the</li> </ul> <p>Test execution of Scenario 2 is expected to stop at this point with errors generated prior to the creation of election media in ballot preparation, however, if no error is displayed continue with the election and verify the application(s) do not crash or have any loss of data.</p> <p>If an error/status message is given, check audit logs messages. Test stops unless system does not error and creates media</p>
Volume:	Same as Volume 1 - Maximum Ballot Styles for paper on the M100; except <ul style="list-style-type: none"> <li>- The system responds to processing more than the expected number of ballot styles in a single precinct</li> </ul>
Stress	System responses to overloading conditions. Exceeding the maximum allowed number of ballot styles in a single precinct.
Performance	Same as Volume 1 - Maximum Ballot Styles for paper on the M100; except <ul style="list-style-type: none"> <li>-When installing an election with 1 precinct and over the maximum number of ballot styles for a give device</li> </ul>
Error Recovery	Same as Volume 1 - Maximum Ballot Styles for paper on the M100; except - the errors are caused by overloading the number ballots styles per precinct.
Readiness Testing and Poll Verification	Same as Volume 1 - Maximum Ballot Styles for paper on the M100; except <ul style="list-style-type: none"> <li>- Test data (run 2 different ballot styles within a precinct to validate the system is ready) is segregated from voting data, with no residual effect'</li> </ul>
Pre-vote: Opening the Polls Verification	Same as Volume 1 - Maximum Ballot Styles for paper on the M100
Voting: Ballot Activation and Casting Verifications	<p>Protects secrecy of ballot/vote</p> <ul style="list-style-type: none"> <li>- Records selections and non-selection of individual choices for each contest</li> <li>- Increment the ballot counter</li> </ul> <p><b>Scenario 1)</b></p> <ul style="list-style-type: none"> <li>- 20 ballots will be test (a 50% sample of 40 ballot styles)</li> <li>- Reuse the ballots for 20 different ballot styles within the deck that were generated on the VAT for the <b>ESSUNITY3200</b> certification effort.</li> <li>- M100- scans the ballots generated by the VAT with different ballot styles within the deck.</li> <li>- Ballot styles 1 through 10, 20 and 40 will be voted</li> <li>- The M100 In Election Day mode with a single precinct and 40 ballot styles will not error. If there are any system errors that cause the M100 to shut down then the M100 shall recover without any loss of data.</li> </ul> <p><b>Scenario 2)</b> Errors should prevent the test from reaching this point. If the test does get to this point:</p> <p>M100</p> <ul style="list-style-type: none"> <li>- Load election on to the M100 containing 41 ballot styles in a singe precinct.</li> <li>- No system failures that cause the M100 to crash or loss data</li> <li>- If there are any system errors that cause the M100 to crash then the M100 shall recover without any loss of data.</li> </ul>
Voting: Voting System Integrity, System Audit,	Same as Volume 1 - Maximum Precincts and Ballot Styles; except -

<b>Method Detail</b>	<b>Volume 2 Test Method</b>
Errors & Status Indicators	report of normal/abnormal events is found within the 50% sample.
Post-vote: Closing the Polls	Once the polls are closed the voting system Same as Volume 1 - Maximum Ballot Styles for paper on the M100; except - <ul style="list-style-type: none"> <li>- M100 Prints a single precinct totals report totaling all ballot styles within the precinct (Election Day voting ends)</li> </ul>
Post-vote: Central Count	Same as Volume 1 - Maximum Ballot Styles for paper on the M100; except <ul style="list-style-type: none"> <li>- View and Print Precinct by Precinct Report for Precinct 1 with 40 ballot styles</li> </ul> <b>Scenario 2)</b> Errors should prevent the test from reaching this point. If the test does get to this point: ERM Same as Volume 1 - Maximum Ballot Styles for paper on the M100; except <ul style="list-style-type: none"> <li>- View and Print Precinct by Precinct Report for Precinct 1 with 41 ballot styles</li> <li>- No system failures that cause the ERM application to crash</li> <li>- If there are any system errors that cause the ERM to crash then the ERM application shall recover without any loss of data.</li> </ul>
Expected Results are observed	Review the test result against the expected result: Same as Volume 1 - Maximum Ballot Styles for paper on the M100
Record observations and all input/outputs for each election;	All inputs, outputs, observations, deviations and any other information impacting the integrity of the test results will be recorded in the test case. Same as Volume 1 - Maximum Ballot Styles for paper on the M100

#### **7.4.2.3 Volume 4 Test Results**

Testing was conducted on the system configuration identified in the PCA Configuration and Test Case. Specific software and firmware builds for each test execution are recorded in the PCA Configuration as identified in the individual test case document.

Date	Test Result	Issues Opened	Issues Closed	Notes
10/1/2009	Reject	# 65		Rev 00 - M100 audit log will not print once the log is full.
2/2/2010	Accept		#65	Rev 01- Verified audit log prints when the log is full

While documentation discrepancies may be encountered in testing they do not result in the rejection of a functional test. Identified issues are found in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#).

<b>Method Detail</b>	<b>Volume 4 Test Method</b>
Test Case Name	Volume 4 - Storage Error Generation
Scope - identifies the type of test	The Test Scope is to test: The M100 component media generate an error messages when capacity is reached without loss of data or data corruption.
Test Objective	The objective is to validate that the M100 provides an error messages when the PCMCIA capacity has been reached and that the PCMCIA card does not become corrupt once the error is displayed nor does the card have any loss of votes or audit log entries.
Test Variables:	A PCB file containing an election definition is loaded on to the PCMCIA card. Using the OMNI drive's PC Card Manager program to copy the PCB file on to the PCMCIA card. The file should be near capacity of the 512 PCMCIA card (for the M100), such that it is close to having the allowable storage full.
A description of the voting system type and the operational environment	The test will only include the M100
VSS 2002 vol. 1	2.2.5.2.2 System Audit Error Messages 2.2.5.2.3 System Audit Status Messages
VSS 2002 vol. 2	A4.3.5 Performance/Recovery (Processing rates-graceful shut down "no system crash" and recovery without loss of data) A4.3.5 Stress (system response to overloading data on hardware media)

<b>Method Detail</b>	<b>Volume 4 Test Method</b>
Hardware, Software voting system configuration and test location	The Unity 3.2.1.0 Voting System consists of the following: 1 @ Model 100 (M100) All testing was performed by iBeta LLC located at 3131 S. Vaughn Way, Aurora, CO 80014.
Pre-requisites and preparation for test case execution	Complete the prerequisites; Test Method Validation: Technical review conducted by C Coggins Approved 9/18/09 for validation of test method as defined in ISO/IEC 17025 clause 5.4.5. Condition of approval - iBeta validates component media is populated to near capacity prior to test execution by viewing the file size using a PC
Getting Started Checks	Check the voting system to: Same as Volume 1 - Maximum Ballot Styles for paper on the M100 - except for the environment. The environment is set up with a Peer to Peer configuration with the OMNI drive's PC Card Manager program.
Documentation of Test Data & Test Results	Test Data: •Same as Volume 1 - Maximum ballot styles for paper on the M100
Volume: Paper-based voting systems Processing	Test Data: •Election media can be installed •There are no system errors that cause the M100 to crash.
Volume:	Not Applicable (only testing for error generation of full media on hardware)
Stress	Not Applicable (only testing for error generation of full media on hardware)
Performance	No system degradation (Ballot Processing rate): - On the M100 with a large amount of data filling up the media storage the system will not be observed to slow down throughout the testing
Error Recovery	The systems should not error or crash. • If the application does error the system shall provide a clear description of the problem.
Readiness Testing and Poll Verification	Not Applicable (only testing for error generation of full media on hardware)
Pre- vote: Opening the Polls Verification	•Same as Volume 1 - Maximum Ballot Styles for paper on the M100
Voting: Ballot Activation and Casting Verifications	M100 Only- Election Day Voting in Polling Place 1 - Zero count report - Using media that is near capacity scan the hand marked ballots - An error "Audit Log Full" is generated. - Error message must advise the official how to handle the error. - If there are any system errors that cause the M100 to crash then verify the M100 will recover without any loss of data.
Voting: Voting System Integrity, System Audit, Errors & Status Indicators	The system audit provides a time stamped, report of normal/abnormal events found within the tested. Error messages are: - Are generated, stored & reported as they occur - Errors requiring intervention by the poll worker clearly display issues & action instructions in easily understood text language or with indicators - Incorrect responses will not lead to irreversible errors.
Post-vote: Closing the Polls	Not Applicable (only testing for error recovery of full media on hardware)
Post-vote: Central Count	Not Applicable (only testing for error recovery of full media on M100 hardware)
Expected Results are observed	Review the test result against the expected result: • Same as Volume 1 - Maximum ballot styles for paper
Record observations and all input/outputs for each election;	All inputs, outputs, observations, deviations and any other information impacting the integrity of the test results will be recorded in the test case. Same as Volume 1 - Maximum ballot styles for paper on the M100

#### 7.4.2.4 Volume 5 Test Results

Date	Test Result	Issues Opened	Issues Closed	Notes
2/15/2010	Accept			

While documentation discrepancies may be encountered in testing they do not result in the rejection of a functional test. Identified issues are found in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#).

Method Detail	Volume 5 Test Method
Test Case Name	Volume 5 - Error Recovery on the M100
Scope - identifies the type of test	<p>The scope is to reuse SysTest M100 Electrical Supply test (2 hour batter error recovery) and iBeta's M100 Volume and Stress testing:</p> <p>Recovery tests verify the ability of the system to recover from hardware and data errors. Power recovery was tested by SysTest in the M100 Electrical Supply Test Case. ES&amp;S has petitioned the EAC for reuse of the applicable components in scope for Unity 3.2.1.0 from the SysTest testing of the Unity v.4.0.0.0 certification test effort. Determination of reuse was based upon the EAC review of SysTest Electrical Supply test results.</p> <p>iBeta incorporates verification of audit logging of error recovery in the Volume Test Cases</p>
Test Objective	<p>Determination by the EAC of the ES&amp;S Unity 4.0.0.0 reuse and the EAC acceptance of the iBeta Volume methods.</p> <p>All Error Recovery testing has been covered throughout the Volume and Electrical Supply testing.</p>
Test Variables: Volume, Stress, Performance, Error Recovery	<p>Test case must have:</p> <p>Verify EAC acceptance of reuse of the "Electrical Supply" test case.</p> <p>Verify all Volume 1, 2, 4, 11 &amp; 12 test steps pass.</p>
A description of the voting system type and the operational environment	The Unity 3.2.1.0 EMS includes a peer-to-peer Network and the M100. Testing includes both reuse of ES&S <b>ESSUNITY3200</b> election databases and creation of new election databases to validate the maximum and exceed the maximum limits.
VSS 2002 vol. 1	Same as Volume 1 - Maximum ballot styles for paper on the M100
VSS 2002 vol. 2	<p>A4.3.5 Stress (high volume with interrupts and overloading the systems)</p> <p>A4.3.5 Recovery (system recovers from software and hardware errors without loss of data)</p>
Hardware, Software voting system configuration & test location	Same as Volume 1 - Maximum ballot styles for paper on the M100
Pre-requisites and preparation for test case execution	<p>iBeta Volume Test Cases must have been executed and passed</p> <p>Determination by the EAC allowing the reuse of SysTest Electrical Supply testing</p>
Getting Started Checks	Not Applicable (Testing is being performed in all iBeta Volume test cases and in the EAC acceptance of the "Electrical Supply test case" reuse tested by SysTest.)
Documentation of Test Data & Test Results	Testing is being recorded in all iBeta Volume test cases and in the determination of EAC acceptance of the "Electrical Supply test case" reuse tested by SysTest.
Volume: Paper-based voting systems Processing	Review SysTest and iBeta Test Cases and validate the following: Vote processing
Volume:	Review SysTest and iBeta Test Cases and validate the following: Overloading systems capacity to process, store, and report data.
Stress	Review SysTest and iBeta Test Cases and validate the following: Software response to power interrupts.
Error Recovery	Review SysTest and iBeta Test Cases and validate the following: Voting system availability to recover gracefully from errors or crashes caused by power failures.
Readiness Testing and Poll Verification	Not Applicable (Testing is being performed in all iBeta Volume test cases and in the EAC acceptance of the "Electrical Supply test case" reuse tested by SysTest.)
Pre- vote: Opening the Polls Verification	Not Applicable (Testing is being performed in all iBeta Volume test cases and in the EAC acceptance of the "Electrical Supply test case" reuse tested by SysTest.)

<b>Method Detail</b>	<b>Volume 5 Test Method</b>
Voting: Ballot Activation and Casting Verifications	Not Applicable (Testing is being performed in all iBeta Volume test cases and in the EAC acceptance of the "Electrical Supply test case" reuse tested by SysTest.)
Voting: Voting System Integrity, System Audit, Errors & Status Indicators	Not Applicable (Testing is being performed in all iBeta Volume test cases and in the EAC acceptance of the "Electrical Supply test case" reuse tested by SysTest.)
Post-vote: Closing the Polls	Not Applicable (Testing is being performed in all iBeta Volume test cases and in the EAC acceptance of the "Electrical Supply test case" reuse tested by SysTest.)
Post-vote: Central Count	Not Applicable (Testing is being performed in all iBeta Volume test cases and in the EAC acceptance of reuse tested by SysTest "Electrical Supply test case".)
Expected Results are observed	Review the test result against the expected result: Same as Volume 1 - Maximum ballot styles for paper
Record observations and all input/outputs for each election;	All inputs, outputs, observations, deviations and any other information impacting the integrity of the test results will be recorded in the test case. Same as Volume 1 - Maximum ballot styles for paper

#### **7.4.2.5 Volume 11 Test Results**

Date	Test Result	Issues Opened	Issues Closed	Notes
9/31/2009	Accept			Scenario 1 & 2

No functional issues were identified. While documentation discrepancies may be encountered in testing they do not result in the rejection of a functional test.

<b>Method Detail</b>	<b>Volume 11 Test Method</b>
Test Case Name	Volume 11 - Maximum number precincts in an early voting polling location on the M100
Scope - identifies the type of test	The scope is to test 450 precincts on 1 PCMCIA card, creating and tally the election on a Peer-to-peer configuration (multiple PCs) set up. <b>Scenario 1)</b> Test the maximum allowed: number of precincts in a single early voting polling location <b>Scenario 2)</b> To verify that errors are generated when: Exceeding the HPM maximum allowed: number of precincts in a single early voting polling location Functional testing of discrepancy #20 in ERM (#104 transferred from <b>ESSUNITY3200</b> )
Test Objective	The objective is to validate the ability to process, store and report data to the maximum and exceeding the maximum allowed number of precincts in a single polling location. The election will be created and tallied on a peer-to-peer configuration (multiple PCs) set up. To validate that the system generates errors during EMS ballot preparation (ballot preparation including: EDM, ESSIM & HPM) when exceeding maximum the allowed number of precincts in a single polling location. Validating the processing, storing and reporting shall occur without system degradation. If there are system errors then the system shall recover without any loss of data.
Test Variables: Volume, Stress, Performance, Error Recovery	General election by Precinct <b>Scenario 1)</b> M100 set up for Early Voting 450 precincts 5 ballot styles 10 contests total (2 contesting per ballot style) 5 candidates per contest (50 total) 5 District Types 5 District Names 10 District Relations 10 Office Relations 11" Ballots (36 oval positions per column, 6 columns, 216 total positions) 2 Statistical Counters (ballots counted and precincts counted) 1 Polling Place set up as an early voting location Contest 1 w/candidates 1 - 5 and 2 w/candidates 6 - 10 in Precincts 1 – 100, ballot style 1

Method Detail	Volume 11 Test Method
	<p>Contest 3 w/candidates 11 - 15 and 4 w/candidates 16 - 20 in Precincts 101,- 200ballot style 2      Contest 5 w/candidates 21 - 25 and 6 w/candidates 26 - 30 in Precincts 201-300, ballot style 3      Contest 7 w/candidates 31 - 35 and 8 w/candidates 36 - 40 in Precincts 301-400, ballot style 4      Contest 9 w/candidates 41 - 45 and 10 w/candidates 46 - 50 in Precincts 401-450, ballot style 5      Discrepancy 20: Set Jurisdiction System Type to "Precinct Count"</p> <p><b>Scenario 2)</b> Same as scenario 1 except:      - 451 precincts</p>
A description of the voting system type and the operational environment	<p>The Unity 3.2.1.0 EMS includes a peer-to-peer Network:      An M100 Precinct Count scanner with 450 precincts in a single Polling Place.</p>
VSS 2002 vol. 1	<p>Same as Volume 1 - Maximum ballot styles for paper on the M100</p>
VSS 2002 vol. 2	<p>A4.3.5 Volume (maximum and exceeding more than the maximum number of precincts in a Polling Place)      A4.3.5 Volume/Stress (Processing, storing and reporting data when overloading the number of precincts in a Polling Place)      A4.3.5 Performance/Recovery (Ballot format handling capability-graceful shut down and recovery without loss of data)      A4.3.5 Performance/Recovery (Processing rates-graceful shut down and recovery without loss of data)</p>
Hardware, Software voting system configuration & test location	<p>Same as Volume 1 - Maximum ballot styles for paper on the M100</p>
Pre-requisites and preparation for test case execution	<p>Complete the prerequisites:      Test Method Validation: Technical review conducted by C Coggins &amp; J Garcia; Approved 9/14/09 for validation of test method as defined in ISO/IEC 17025 clause 5.4.5.</p> <p>Import Wizard method validation completed in <b>ESSUNITY3200</b>      - Excel spreadsheets saved as "Tab Delimited". Tab Delimited documents containing election creating information will be imported into EDM using the Import Wizard option.</p> <p>Spreadsheet 1 - Precincts 450 and 451      Spreadsheet 2 - District Types 5      Spreadsheet 3 - Districts Names 5      Spreadsheet 4 - District Relations 5      Spreadsheet 5 - Master Office 10      Spreadsheet 6 - Office Relations 10      Spreadsheet 7 - Candidates 50</p>
Getting Started Checks	<p>Test Data:      Same as Volume 1 - Maximum Ballot Styles for paper on the M100</p>
Documentation of Test Data & Test Results	<p>Test Data:      Same as Volume 1 - Maximum Ballot Styles for paper on the M100</p>
Volume: Paper-based voting systems Processing	<p>Ballot Prep:      -An election database can be accurately/securely defined &amp; formatted using the Import Wizard.      -Ballots (candidates) can be accurately defined &amp; generated.</p> <p><b>Scenario 1)</b>      Election can be created and installed with 450 Precincts in a single Early Voting poll location. No error occurs - If there are any system errors that cause the EMS ballot preparation applications to crash then verify the applications recover without any loss of data. - Review the EDM, ESSIM and HPM reports to verify election set up.</p> <p><b>Scenario 2)</b>      Same as scenario 1 except over the maximum allowed number of Precincts in a single Early Voting poll location (451). Test execution of Scenario 2 is expected to stop at this point with errors generated in the ballot preparation prior to the creation of election media      - Check audit logs for critical status messages. Test stops unless system does not error and creates</p>

Method Detail	Volume 11 Test Method
	<p>media)</p> <ul style="list-style-type: none"> <li>- If EDM does not error during the "Ballot Sets Merge" then the EDM reports must be reviewed to verify 451 precincts have been created and assigned to a single early voting Polling Place. Continue to ESSIM and HPM. The system should display a critical status message prior to exiting the HPM.</li> <li>- If there are any system errors that cause the EMS ballot preparation applications to crash then verify the applications recover without any loss of data. If no error is given prior to leaving HPM continue the test.</li> </ul>
Volume:	<p>Overloading systems capacity to process, store, and report data.</p> <ul style="list-style-type: none"> <li>- When importing over the allowed amount of data into the EDM using the Import Wizard</li> <li>- Overloading the HPM with more than the allowed number of precincts in a single polling place.</li> </ul>
Stress	<p>System responses to overloading conditions, exceeding the maximum allowed number of Early Voting precincts in a single Polling location.</p>
Error Recovery	<p>There is no system degradation (Ballot format handling capability and Processing rates):</p> <ul style="list-style-type: none"> <li>- When importing large amount of data into the EDM using the Import Wizard.</li> <li>- The system does not slow down throughout the testing</li> </ul>
Readiness Testing and Poll Verification	<p>Same as Volume 1 - Maximum ballot styles for paper on the M100</p>
Pre- vote: Opening the Polls Verification	<p>Voting system is ready for the election:</p> <p>Same as Volume 1 - Maximum Precincts Limitations and ballot styles for paper except:</p> <ul style="list-style-type: none"> <li>- Run 2 precincts to validate the system is ready; confirm the test data is segregated from voting data, with no residual effect. Verify totals and audit logs.</li> </ul>
Voting: Ballot Activation and Casting Verifications	<p>Precinct Count/ Paper based:</p> <ul style="list-style-type: none"> <li>• Same as Volume 1 - Maximum ballot styles for paper on the M100</li> </ul>
Voting: Voting System Integrity, System Audit, Errors & Status Indicators	<p><b>Scenario 1) Early Voting</b></p> <ul style="list-style-type: none"> <li>- M100 is set up for Early Voting and has all Precincts 1-450.</li> <li>- Voting using 90 different precincts (20% of 450 precincts), 18 ballots per ballot style, ballot styles 1-4 have 100 precincts and ballot style 5 has 50 precincts, each style has 2 contests. A total of 90 ballots will be voted.</li> <li>- Hand mark ballots all but 10% of the ballots</li> <li>- Mark 10% of the ballots using the VAT</li> <li>- Scan using the M100</li> <li>- No errors are expected.</li> <li>- If there are any system errors that cause the M100 &amp; the VAT to crash then verify the M100 and the VAT recover without any loss of data.</li> <li>- Verify the counter (number of voters) on the M100 and the VAT match the expect results.</li> </ul> <p><b>Scenario 2)</b></p> <p>Errors should prevent the test from reaching this point. If the test does get to this point:</p> <ul style="list-style-type: none"> <li>- Load election</li> <li>- No system failures that cause the M100 and/or the VAT to crash</li> <li>- If there are any system errors that cause the M100 and the VAT to crash then the M100 and the VAT shall recover without any loss of data.</li> </ul>
Post-vote: Closing the Polls	<p>Same as Volume 1 - Maximum ballot styles for paper on the M100</p>
Post-vote: Central Count	<p>Once the polls are closed the voting system</p> <ul style="list-style-type: none"> <li>- Printed reports of ballots counted by tabulator</li> <li>- The reported votes match the predicted votes for the tabulator with votes and undervotes.</li> <li>- In the Early Voting Poll location prints the M100 summary report with all 450 precincts (early voting ends)</li> </ul>
Expected Results are observed	<p><b>Scenario 1)</b></p> <p>The (ERM) central count voting system:</p> <p>Discrepancy 20: Setting "Precinct Count" in HPM does not cause an error in ERM "Error: File: "TC name" CTR, Error: #35 - File does not exist." The election cannot proceed".</p>

Method Detail	Volume 11 Test Method
	<ul style="list-style-type: none"> <li>- Discrepancy 20: verify no error " "Convert Precinct Results File: The precincts results file is from older software and is being converted." and "Error: File: Vol8S1.CTR, Error: #35 - File does not exist." is displayed when attempting to re-launch ERM.</li> <li>- Correctly displays the Election</li> <li>- Print a Zero count report (to verify no votes have been updated into the ERM prior to starting consolidation)</li> <li>- No errors are expected.</li> <li>- If there are any system errors that cause the ERM to crash then the system shall recover without any loss of data.</li> </ul> <p>Vote Consolidation:</p> <ul style="list-style-type: none"> <li>- ERM consolidated reports match the predicted votes.</li> <li>- Verify no data was lost within the audit logs or results</li> </ul> <p>Reports include:</p> <ul style="list-style-type: none"> <li>- Printed reports of ballots counted by tabulator, with votes and undervotes <ul style="list-style-type: none"> <li>- Print the Summary Report</li> <li>- View and Print Precinct by Precinct Reports</li> </ul> </li> </ul> <p><b>Scenario 2)</b> Errors should prevent the test from reaching this point. If the test does get to this point:</p> <ul style="list-style-type: none"> <li>- continue to the ERM - No system failures that cause the EMS ERM application to crash - If there are any system errors cause the EMS ERM application to crash then the ERM application shall recover without any loss of data.</li> </ul>
Record observations and all input/outputs for each election;	<p>Review the test result against the expected result:</p> <ul style="list-style-type: none"> <li>• Same as Volume 1 - Maximum ballot styles for paper on the M100</li> </ul>

#### 7.4.2.6 Volume 12 Test Results

Date	Test Result	Issues Opened	Issues Closed	Notes
9/28/2009	Halted			Rev 00 for Scenario 1 and 2 Stopped execution of testing due to error in election set up. Modifications were made in Rev 1 for both Scenario 1 & 2.
9/30/2009	Accept			Rev 1 Scenario 1
10/2/2009	Reject	# 67		Rev 1 Scenario 2; No error message is generated when an election with 19 precincts is assigned in HPM (system limit for M100 is 18 precincts).
2/2/2010	Reject	#67		Rev. 2- Scenario 2; Warning message is generated when a 19th precinct is created in HPM but not when it is created in EDM and imported into HPM
2/15/2010	Accept		#67	Rev. 3- Scenario 2- HPM warning is generated for 19 precincts

While documentation discrepancies may be encountered in testing they do not result in the rejection of a functional test. Identified issues are found in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#).

Method Detail	Volume 12 Test Method
Test Case Name	Volume 12 - Maximum number precincts in an polling place polling place.
Scope - identifies the type of test	<p>The scope is to test 18 precincts on 1 PCMCIA card, create and tally the election on a Peer to Peer configuration (multiple PCs) set up.</p> <p><b>Scenario 1)</b> Test the M100 maximum allowed: number of Election Day precincts in a single polling place in handled on the M100</p> <p>To verify that errors are generated when:</p> <p><b>Scenario 2)</b> In HPM when exceeding the M100 maximum allowed: number of Election Day precincts in a single polling Place.</p>
Test Objective	The objective is to validate the ability to process, store and report data to the M100 maximum and exceeding the maximum allowed number of precincts in a single polling place. The election will be created and tallied on a Peer to Peer configuration (multiple PCs) set up. To validate that the system generates errors during EMS ballot preparation (ballot preparation including: EDM, ESSIM &

<b>Method Detail</b>	<b>Volume 12 Test Method</b>
	HPM) when exceeding maximum the allowed number of precincts in a single polling place. Validating the processing, storing and reporting shall occur without system degradation. If there are system errors then the system shall recover without any loss of data.
Test Variables: Volume Stress Performance Error Recovery	Closed Primary by style Election Day voting <b>Scenario 1)</b> 2 parties 18 precincts 2 ballot styles (1 for REP and 1 for DEM) each will be included in all 18 precincts. 6 contests total (2 partisan and 4 non partisan) 10 candidates per contest (total of 60) Vote for 1 and 2 candidates (1 Partisan and 1 Non-Partisan = Vote for 1 and 1 Partisan and 3 Non-Partisan = Vote for 2) Write-Ins on each of the contests 5 District Types 5 District Names 5 District Relations 6 Office Relations 17" Ballots (45 oval positions per column, 6 columns, 270 total positions) 2 Statistical Counters 1 Polling Place <b>Scenario 2)</b> Same as scenario 1 except: - 19 precincts
A description of the voting system type and the operational environment	The Unity 3.2.1.0 EMS includes a Peer to Peer Network: An M100 Precinct Count scanner with 18 precincts in a single Polling Place and using a Peer to Peer PC configuration.
VSS 2002 vol. 1	• Same as Volume 1 - Maximum ballot styles for paper on the M100
VSS 2002 vol. 2	A4.3.5 Volume (maximum and exceeding more than the maximum number of precincts in a Polling Place) A4.3.5 Volume/Stress (Processing, storing and reporting data when overloading the number of precincts in a Polling Place) A4.3.5 Performance/Recovery (Ballot format handling capability-graceful shut down and recovery without loss of data) A4.3.5 Performance/Recovery (Processing rates-graceful shut down and recovery without loss of data)
Hardware, Software voting system configuration and test place	Same as Volume 1 - Maximum Ballot Styles for paper on the M100
Pre-requisites and preparation for execution of the test case.	Complete the prerequisites: Test Method Validation: Technical review conducted by Carolyn Coggins Approved 9/17/09 for validation of test method as defined in ISO/IEC 17025 clause 5.4.5. Import Wizard method tested and validated in <b>ESSUNITY3200</b> certification test effort - Excel spreadsheets saved as "Tab Delimited". Tab Delimited documents containing election creating information will be imported into EDM using the Import Wizard option. Spreadsheet 1 - Precincts 18 and 19 Spreadsheet 2 - District Types 5 Spreadsheet 3 - Districts Names 5 Spreadsheet 4 - District Relations 5 Spreadsheet 5 - Master Office 6 Spreadsheet 6 - Office Relations 6 Spreadsheet 7 - Candidates 60
Getting Started Checks	• Same as Volume 1 - Maximum ballot styles for paper on the M100
Documentation of Test Data & Test Results	• Same as Volume 1 - Maximum ballot styles for paper on the M100
Volume: Paper-based voting systems Processing	Ballot Prep: -An election database can be accurately/securely defined & formatted using the Import Wizard. -Ballots (candidates) can be accurately defined & generated.

Method Detail	Volume 12 Test Method
	<p><b>Scenario 1)</b> Election can be created and installed with 18 Precincts in a single polling place poll place. No error occurs To verify that errors are generated when:- If there are any system errors that cause the EMS ballot preparation applications to crash then verify the applications recover without any loss of data.</p> <ul style="list-style-type: none"> <li>- Review the EDM, ESSIM and HPM reports to verify election set up.</li> </ul> <p><b>Scenario 2)</b> Same as scenario 1 except over the maximum allowed number of Precincts in a single polling place poll place (19). (ENH17702 Disc #67)</p> <p>Test execution of Scenario 2 is expected to stop at this point with errors generated in the ballot preparation prior to the creation of election media - Check audit logs for critical status messages. Test stops unless system does not error and creates media)</p> <ul style="list-style-type: none"> <li>- If EDM does not error during the "Ballot Sets Merge" then the EDM reports must be reviewed to verify 19 precincts have been created and assigned to a single polling place. Continue to ESSIM and HPM. The system should display a critical status message prior to exiting the HPM.</li> <li>- If there are any system errors that cause the EMS ballot preparation applications to crash then verify the applications recover without any loss of data. If no error is given prior to leaving HPM continue the test.</li> </ul>
Volume:	Overloading systems capacity to process, store, and report data. <ul style="list-style-type: none"> <li>- When importing over the allowed amount of data into the EDM using the Import Wizard</li> <li>- Overloading the HPM with more than the allowed number of precincts in a single polling place.</li> </ul>
Stress	System responses to overloading conditions. Exceeding the maximum allowed number of polling place precincts in a single Polling place.
Performance	There is no system degradation (Ballot format handling capability & Processing rates): <ul style="list-style-type: none"> <li>- When importing large amount of data into the EDM using the Import Wizard.</li> <li>- The system does not slow down throughout the testing</li> </ul>
Error Recovery	<ul style="list-style-type: none"> <li>• Same as Volume 1 - Maximum ballot styles for paper on the M100</li> </ul>
Readiness Testing and Poll Verification	Voting system is ready for the election: <ul style="list-style-type: none"> <li>• Same as Volume 1 - Maximum ballot styles for paper on the M100</li> <li>- Run 1 precinct to validate the system is ready; confirm the test data is segregated from voting data, with no residual effect.</li> <li>- Verify totals and audit logs.</li> </ul>
Pre- vote: Opening the Polls Verification	Precinct Count/ Paper based: <ul style="list-style-type: none"> <li>• Same as Volume 1 - Maximum ballot styles for paper on the M100</li> </ul>
Voting: Ballot Activation and Casting Verifications	<p><b>Scenario 1)</b> A polling place</p> <ul style="list-style-type: none"> <li>- M100 is set up for polling place and has all Precincts 1-18.</li> <li>- Voting using 36 ballots, 2 ballots per ballot style</li> <li>- Hand mark ballots all but 10% of the ballots</li> <li>- Mark 10% of the ballots using the VAT</li> <li>- Scan using the M100</li> <li>- No errors are expected.</li> <li>- If there are any system errors that cause the M100 &amp; the VAT to crash then verify the M100 and the VAT recover without any loss of data.</li> <li>- Verify the counter (number of voters) on the M100 and the VAT match the expect results.</li> </ul> <p><b>Scenario 2)</b> Errors should prevent the test from reaching this point. If the test does get to this point:</p> <ul style="list-style-type: none"> <li>- Load election</li> <li>- No system failures that cause the M100 and/or the VAT to crash</li> <li>- If there are any system errors that cause the M100 and the VAT to crash then the M100 and the VAT shall recover without any loss of data.</li> </ul>
Voting: Voting System Integrity, System Audit, Errors & Status Indicators	Same as Volume 1 - Maximum Ballot Styles for paper on the M100
Post-vote: Closing the Polls	Once the polls are closed the voting system <ul style="list-style-type: none"> <li>- Printed reports of ballots counted by tabulator</li> <li>- Votes reported match the predicted votes from tabulator with votes and undervotes.</li> <li>- In the polling place Poll place print the M100 summary report with all of the 450 precincts (polling place ends)</li> </ul>
Post-vote:	<b>Scenario 1) :</b> The (ERM) central count voting system:

Method Detail		Volume 12 Test Method
Central Count		<ul style="list-style-type: none"> <li>- Correctly displays the Election</li> <li>- Print a Zero count report (to verify no votes have been updated into the ERM prior to starting consolidation)</li> <li>- No errors are expected.</li> <li>- If there are any system errors that cause the ERM to crash then the system shall recover without any loss of data.</li> </ul> <p>Vote Consolidation: ERM consolidated reports match the predicted votes</p> <ul style="list-style-type: none"> <li>- Verify no data was lost within the audit logs or results</li> </ul> <p>Reports include:</p> <ul style="list-style-type: none"> <li>- Printed reports of ballots counted by tabulator, with votes and undervotes</li> <li>- Print the Summary Report</li> <li>- View and Print Precinct by Precinct Reports</li> </ul> <p><b>Scenario 2)</b> Errors should prevent the test from reaching this point. If the test does get to this point:</p> <ul style="list-style-type: none"> <li>- continue to the ERM</li> <li>- No system failures that cause the EMS ERM application to crash</li> <li>- If there are any system errors cause the EMS ERM application to crash then the ERM application shall recover without any loss of data.</li> </ul>
Expected Results are observed		<p>Review the test result against the expected result:</p> <ul style="list-style-type: none"> <li>• Same as Volume 1 - Maximum ballot styles for paper on the M100</li> </ul>
Record observations and all input/outputs for each election;		<p>All inputs, outputs, observations, deviations and any other information impacting the integrity of the test results will be recorded in the test case.</p> <ul style="list-style-type: none"> <li>• Same as Volume 1 - Maximum ballot styles for paper on the M100</li> </ul>

#### 7.4.2.1 Volume 13 Test Results

Date	Test Result	Issues Opened	Issues Closed	Notes
5/04/2010	Accept			

Method Detail		Volume 13 Test Method
Test Case Name		Volume 13 - 65500 ERM Precinct Element Limitation
Scope - identifies the type of test		To evaluate ES&S testing of 65,500 ERM Precinct Element limitation and exceeding the maximum limitation, with an independent iBeta validation that ERM handles the test election data.
Test Objective		<p>To examine and evaluate the adequacy of the testing performed by ES&amp;S in the ES&amp;S TC (ERM Limit 65500 Test Case) to verify the 65,500 ERM Precinct Element limit.</p> <p>Based on the findings of the examination and evaluation iBeta will determine if the documentation and internal test results provided by ES&amp;S acceptably demonstrate that the limit was tested, the test verified the maximum limit could be reached with election results correctly reported and exceeding the limit was handled by ERM iBeta will independently verify the election data is read in ERM.</p>
Test Variables: Volume Stress Performance Error Recovery		<p>Review ES&amp;S test case to verify:      ES&amp;S has defined an "ERM Precinct Element"      General Election      Ballot Set Ballot ID is By Precinct      Statistical Counters include Ballots Counted Total      1 Polling Place will include all Precincts      Ballot Size is 14" 36 rows</p>
A description of the voting system type and the operational environment		Verify ES&S performed the test on the Unity 3.2.1.0 EMS and with the DS200 Precinct Count scanner
VSS 2002 vol. 1		<p>Review the ES&amp;S test case and verify that it documents the testing of the following requirements:</p> <ul style="list-style-type: none"> <li>2.2.5.2 Audit/Error messages</li> <li>2.2.5.2.3 Audit/Status messages</li> <li>2.2.3 Error Recovery</li> </ul>
VSS 2002 vol. 2		<p>Review the ES&amp;S test case and verify that it documents the testing of the following requirements:</p> <ul style="list-style-type: none"> <li>A4.3.5 Volume (maximum and exceeding more than the maximum number of precincts elements)</li> <li>A4.3.5 Volume/Stress (Processing, storing and reporting data when overloading the number of precincts elements)</li> <li>A4.3.5 Recovery (report handling capability-graceful shut down and recovery without loss of data)</li> </ul>

<b>Method Detail</b>	<b>Volume 13 Test Method</b>
	A4.3.5 Recovery (Processing rates-graceful shut down and recovery without loss of data) 6.7 Functional Configuration Audit
Hardware, Software voting system configuration and test place	Review the ES&S test case and verify: The hardware and software configuration includes: The Unity 3.2 Voting System consist of the following: Audit Manger (AM ), Election Data Manger (EDM), (ESSIM), hardware Program Manger (HPM), DS200, Election Reporting Manager (ERM) and the ES&S test location, tester and test date is documented  ERM installed on the Unity 3.2.1.0 iBeta test platform
Pre-requisites and preparation for execution of the test case.	Review the test data in the test case to confirm it meets the definition of ERM Precinct Element. Obtain the executed ES&S test case and the election archive  Load the election archive on the iBeta test platform
Getting Started Checks	Check the test case and version of ERM to confirm it is the same as the Trusted Build install on the iBeta test platform
Documentation of Test Data & Test Results	Test Data: •iBeta will accept the ES&S test results if: 1) The test case documents that the ERM Precinct Element limit was tested, the test verified the maximum limit could be reached with election results correctly reported and exceeding the limit was handled by ERM 2) All steps have passed
Volume: Paper-based voting systems Processing	Verify the test cases documents ES&S created the elections with the " Test Variables" (see above)
Volume:	Review and verify the ES&S test case confirms: •The systems can process, store, and report 65500 precinct elements within a single contest
Stress	Review and verify the ES&S test case confirms: •They system provides a response to overloading condition: Exceeding 65500 precinct elements within a single contest
Performance	Review and verify the ES&S test case confirms: No system degradation reading in 65500 precinct elements for a single contest
Error Recovery	Review and verify the ES&S test case confirms: Verify the ES&S ERM Precinct Element Limitation test case • If the ERM errors when exceeding 65500 precinct elements within a single contest, ES&S confirmed ERM gracefully shuts down (no crash) and recovers from errors caused by the overload without loss of data. •If ERM does not error confirm the system can process, store and report a number exceeding 65500 by at least 1.
Readiness Testing and Poll Verification	Review and verify the ES&S test case includes: Correct installation of the election on the DS200
Pre- vote: Opening the Polls Verification	Review and verify the ES&S test case includes: Opening the polls and running a zero report on the DS200
Voting: Ballot Activation and Casting Verifications	Review and verify the ES&S test case includes: <b>Scenario 1</b> 3275 ballots were scanned (each contest is a vote for 20, 1 candidate is voted on each contest leaving 19 undervotes for each contest for a total of 65500 precinct elements) <b>Scenario 2</b> 3276 ballots are scanned (each contest is a vote for 20, 1 candidate is voted on each contest leaving 19 undervotes for each contest for a total of 65520 precinct
Voting: Voting System Integrity, System Audit, Errors & Status Indicators	Review and verify the ES&S test case includes: Verifying the required number of ballots are scanned
Post-vote: Closing the Polls	Review and verify the ES&S test case includes: Close the polls and running the results report on the DS200
Post-vote:	Review and verify the ES&S test case includes:

<b>Method Detail</b>	<b>Volume 13 Test Method</b>
Central Count	<p><b>Scenario 1</b> 65500 precinct elements "total" was read into the ERM without any errors.</p> <p><b>Scenario 2</b> 65520 precinct elements "total" was read into the ERM without any errors.</p> <p>iBeta loads the Elecdata folder into ERM and confirms the totals match the ES&amp;S documented test results.</p>
Expected Results are observed	Review the test result against the expected result: <ul style="list-style-type: none"> <li>• Same as Volume 1 - Maximum ballot styles for paper on the M100</li> </ul>
Record observations and all input/outputs for each election;	All inputs, outputs, observations, deviations and any other information impacting the integrity of the test results will be recorded in the test case. <ul style="list-style-type: none"> <li>• Same as Volume 1 - Maximum ballot styles for paper on the M100.</li> </ul>

### 7.4.3 FCA Security Review and Testing

During the initial Security Document Review conducted 8/18/2009 through 9/25/2010 test criteria was identified. Security testing or reviews (source code or document) were broken down into unique security tests/reviews or test/reviews already addressed in standard testing and document or source code reviews. Unique security tests, source code, or document reviews are identified in 7.4.3. Test results for the standard tests, source code, or document reviews are identified in those sections. Security Testing was performed on the system configuration identified in the PCA Configuration and section 3.

Date	Test Result	Issues Opened	Issues Closed	Notes
9/8/09	Reject	35, 54 & 61		Sec Doc Rev 0
9/8/09	Reject	7, 25, 42, 44, 45, 52, 53, 55-60, 78-79, 84, 86, 91, 92		Sec Test Rev 0 Issue 7 - Functionality "counterfeit ballot detection" was withdrawn per ES&S
10/12/09	Reject	81		3210 Regression Test Steps
10/15/09	Reject	75		Network Ports - P2P Rev 0
10/15/09	Reject	70 - 73, 88, 89, 90 & 93		Win Conf - Client Server Rev 0
10/15/09	Reject	72 -75		Win Conf - E077(P2P) Rev 0
10/15/09	Accept			Network Ports - Client Server Rev 0
2/3/10	Reject	103, 117, 118, 119	25, 52, 53, 55, 57, 58, 60	Sec Test Rev 1 New Hardening Procedures arrived testing was stopped and a new Rev was added to address the new discrepancies as well as the following: 42, 44, 45, 56, 59, 78-79, 84, 86, 91-92
2/3/10 & 2/18/10	Reject	117, 118	72 -74	Win Conf - Alone Rev0 Win Conf - E077(P2P) Rev 1 Hardening Procedures document dated 2/8/10
2/8/10	Reject	119		Sec Test Rev1
2/19/10	Accept		75	Network Ports - P2P Rev 1
2/19/10	Accept		117, 118	Win Conf - Alone Rev1 Win Conf - E077(P2P) Rev 2 Hardening Procedures document dated 2/18/10
3/2/10 - 4/15/10	Reject	91& 103 (reopened)	42, 44, 45, 56, 59, 78-79, 84, 86, 92, 103, 117, 118	Sec Test Rev 2 On 3/15 Issue 103 was closed, however, it was reopened on 4/13/2010. Issue 136 was closed (removing security procedures from HPM & ERM). These security procedures were how issue 103 was closed. Removal of the security procedures forced issue 103 to be reopened.
3/20/10	Reject	136		3210 Regression Test Steps Rev 1
4/1/10	Accept		136	3210 Regression Test Steps Rev 3
4/7/10 - 4/14/10	Accept		70 • 73, 88, 89, 90 & 93	Win Conf - Client Server Rev 1
4/7/10	Accept		119	Sec Test Rev 2
4/14/10	Accept			Network Ports - Client Server Rev 1 New Hardening Procedures required further Network port testing.
5/7/10	Accept		35, 54 & 61	Sec Doc Rev 1
5/7/10	Accept		35 & 60	Sec Source Rev 1
5/10/10	Accept		91	Sec Test Rev 3
6/14/10	Reject	160-163		Sec Test Rev 4 Integrity of input blocks of data not validated against the CRC
8/6/10	Accept		81	Test Steps S1 REV03

Date	Test Result	Issues Opened	Issues Closed	Notes
8/11/10	Reject	174		Identified with documentation issue #173
8/11/10	Accept		160-163	Sec Test Rev 5
9/7/10	Accept		174	Verified with documentation issue #173
10/8/10	Reject	HALT 1-82		HALT Source Code Review 1.4.3.6b
10/16/10	Reject	HALT 83-85	HALT 1-78, 81, 82	HALT Source Code Review 1.4.3.6c
10/29/10	Accept		HALT 79, 80, 83, 84, 85	HALT Source Code Review 1.4.3.6d
11/11/10	Reject	189 & 190		Sec Test Rev 6 (Halt Functional test)
12/13/10	Not Tested			Sec Test Rev 7 (Halt Functional test) has not been executed as of 11/29/10 because code to fix 189 & 190 has not been delivered.

Identified issues are found in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#).

Method Detail	Security Test Method
Test Case Name	Security Review and Test Case
Scope • identifies the type of test	Security testing crosses into several areas of voting system testing and thus must be tested at the integrated system level. System Level Tests are customized for the specific voting system to test the security elements incorporated into the Pre-vote, voting and post voting functions. Further examination is performed in Telephony and Cryptographic Tests. A review of the security documentation addresses Access Controls, Physical Security and Software Security.
Test Objective	The objective of security testing is to minimize the risk of accidents, inadvertent mistakes and errors; protect from intentional manipulation, fraud or malicious mischief;
Test Variables:	In the general and primary elections validate the security of the Pre-vote, voting, and post voting functions of the voting system by test incorporating overflow conditions, boundaries, password configurations, negative testing, inputs to exercise errors and status messages, protection of the secrecy in the voting process and identification of fraudulent or erroneous changes. Including: Unauthorized changes to system capabilities for: <ul style="list-style-type: none"> <li>• Defining ballot formats,</li> <li>• Casting and recording votes,</li> <li>• Calculating vote totals consistent with defined ballot formats,</li> <li>• Reporting vote totals,</li> <li>• Alteration of voting system audit trails,</li> <li>• Changing or preventing the recording of a vote,</li> <li>• Introducing data not cast by an authorized voter,</li> <li>• Changing calculated vote totals,</li> <li>• Preventing access to vote data, including individual votes and vote totals, to unauthorized individuals, and</li> <li>• Preventing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes cast by the voter.</li> </ul>
A description of the voting system type and the operational environment	Same equipment and apparatus as the <b>ESSUNITY3200</b> certification except for the addition of: M100: Precinct count based, voter-activated paper ballot counter and vote tabulator. May also be used in a central count location as a ballot counter and vote tabulator. Addition of multiple workstations connected over a LAN in both election preparation and election reporting locations.
VSS 2002 vol. 1	2.2.1, 2.2.4 thru 2.2.5.2.3, 6.2 thru 6.4
VSS 2002 vol. 2	6.4 thru 6.4.2
Hardware, Software voting system configuration and test location	This security test is an incremental change to the <b>ESSUNITY3200</b> certified voting system. The configuration includes the same election preparation and central count applications and devices certified in the <b>ESSUNITY3200</b> configurations. The subsystems included in that certification include EDM (election definition), AIMS (VAT election definition and ballot preparation), ESSIM (ballot preparation), AM (auditing for EDM, ESSIM), HPM and ERM (central count reporting) as well as the voting devices DS200 (precinct scanner), VAT (precinct ballot marking device), and M650 (central count scanner). In addition the M100 acting as either a precinct scanner or

Method Detail	Security Test Method
	<p>central count scanner is added to this certification. This certification also differs from the <b>ESSUNITY3200</b> certification by the addition of a LAN to both the election definition location and central count location. No voting devices are connected to the LAN. All deployments are performed by the physical transport of memory devices consistent with the <b>ESSUNITY3200</b> certification.</p> <p>Configuration 1 (peer-to-peer) Multiple Windows XP SP3 workstations are connected over a LAN. This configuration may also include a network printer.</p> <p>Configuration 2 (domain) Multiple Windows XP SP3 workstations are connected on a LAN that includes a Windows 2003 fileserver (or domain server). This configuration may also include a network printer.</p> <p>Configuration 3 (stand alone) A single Windows XP SP3 computer not connected to any network.</p> <p>Ballot definition (EDM) and ballot preparation (ESSIM) applications may share the network but are procedurally prevented from accessing the same election over the network. Ballot definition deployment (HPM) applications are procedurally prevented from modifying any ballot definitions in a network but are allowed read-only access to ballot definitions to facilitate large deployments. Multiple election reporting workstations may share the election results database to share reporting tasks.</p>
Pre-requisites and preparation for execution of the test case.	<p>The System Level and Telephony and Cryptographic Test Cases are reviewed to ensure that they incorporate the security test requirements and the procedural requirements identified in the vendor supplied security documentation.</p> <ul style="list-style-type: none"> <li>• Additional tests, not covered in the System Level Test Cases are performed as applicable for the security requirements of the system.</li> <li>• COTS applications necessary for PC hardening are downloaded or otherwise obtained and validated.</li> <li>• Configurations described above are prepared. COTS PC's are hardened as per vendor documentation and appropriate election applications are loaded.</li> <li>• As necessary to test bit error detection and error handling for the M100 and DS200, prepare an election. This election is the base case for testing bit error detection and error handling as it occurs between the HPM and scanning device. The base election is also voted with known ballots and used to test the bit error detection and error handling within ERM as it occurs between the voting device and the ERM.</li> </ul>
Getting Started Checks	<p>Prior to testing Verify the following through Document Review</p> <ul style="list-style-type: none"> <li>• M100 documentation contains instructions to physically protect the PC cards during and following an election.</li> <li>• M100 documentation contains security provisions that are compatible with the procedure and administrative tasks involved in equipment preparation, testing, and operation.</li> <li>• M100 documentation contains mandatory administrative procedures for effective system security.</li> <li>• Documentation specifies usage of tamper-evident seals to protect the modem, PC card slot(s), serial ports, polls open/close switch, and printer compartment during polls open, and to protect the firmware at all times after it is loaded with a trusted build. (NY 7/12/07) &amp; (CT 10/1/06 &amp; 7/1/07)</li> <li>• M100 documentation includes maintaining the zeroization report as part of the official audit record</li> <li>• M100 manual identifies access control security measures including software, hardware, communication, password management, operating system provided controls, supervisor privileges, and segregation of duties <ul style="list-style-type: none"> <li>• M100 documentation contains procedures for recovering from a failure of a memory component or data processing component.</li> </ul> </li> <li>• M100 documentation contains procedures for handling the failure of any data input or storage device.</li> <li>• M100 documentation contains procedures for installation of software including hardware containing firmware.</li> <li>• Documentation contains procedures for the secure handling of ballot boxes and data in central count.</li> <li>• Documentation contains procedures for the physical security and detection of tampering in polling places. (CT 10/1/06 &amp; 7/1/07)</li> <li>• Documentation contains detailed description of physical access control measures to prevent unauthorized access to the voting system.</li> </ul>

Method Detail	Security Test Method
	<ul style="list-style-type: none"> <li>• During trusted build procedures and installation, verify source code, compilers or assemblers are not resident.</li> <li>• Documentation states that jurisdictional procedures control multiple user access to election definition files in EDM, ESSIM, AM and AIMS.</li> <li>• Documentation states that jurisdictional procedures control multiple user access to election definition files in HPM. Multiple user access to HPM files is "read-only" during preparation of election definition cartridges for M100, DS200, M650 and VAT.</li> <li>• By document review verify that the multiple user access capabilities of ERM are documented sufficiently to allow a code reviewer to verify and analyze the multi-user capabilities of ERM users.</li> <li>• By source code review M100 validates checksums when the PC card is input</li> <li>• By source code review M100 memory is zeroed out prior to election</li> <li>• By source code review computer generated keys are random</li> <li>• By source code review multiuser access in ERM prevents data corruption, deadlocks, and race conditions.</li> </ul>
Documentation of Test Data & Test Results	<p>Record the results of the security testing in the Security test case. Summarize and record the results of security testing, document &amp; source code reviews in the applicable Security Review tabs.</p> <p>Enter Accept against each review requirement.</p> <p>Log discrepancies on the appropriate Discrepancy Report</p>
Pre-vote: Ballot Preparation procedures verifications	<p>Follow steps in the System Level, and Security Test Cases.</p> <ul style="list-style-type: none"> <li>• Performing windows hardening tests on Windows XP and Windows 2003 in a network enabled configuration including <ul style="list-style-type: none"> <li>• cannot boot to CD or USB devices (<a href="#">KV-124 NY 7/12/07</a>)</li> <li>• non-administrators cannot install applications</li> <li>• users cannot make undetected modifications to election software or data</li> <li>• non-administrators cannot execute non-election related applications</li> <li>• non-administrators cannot clear windows event logs</li> <li>• windows login authentication is required on the terminal</li> <li>• windows event logs contain user login information and user access to applications and objects</li> <li>• disabling the Windows Event Log will halt operation of all election management system applications (test in all EMS network configurations)</li> <li>• verify that the terminal meets best-practice configuration requirements</li> <li>• no source code or compilers are present</li> <li>• perform network penetration testing on network ports</li> <li>• verify that any built-in wireless or modems are inaccessible during voting</li> <li>• verify that HPM requires a non-default password be set in the M100 memory card in order to re-open the polls</li> </ul> </li> <li>• Election definition files transferred by memory device to the DS200 and M100 are validated for integrity using CRC or better and each CRC-protected block of data is validated.</li> </ul>
Pre-vote: Ballot Preparation Security	<ul style="list-style-type: none"> <li>• A guest user or an anonymous user is not allowed access to voting software or data files.</li> <li>• For all networked systems (ESSIM,EDM,HPM,AIMS,AM and ERM) different non-administrative users who would not normally have access to files cannot access critical system files over the network and make undetected modifications to their content.</li> <li>• Unplugging network cables during ballot definition does not irreversibly affect these operations or lead to corrupted output files (EDM,ESSIM,HPM,AIMS).</li> </ul>
Readiness Testing and Poll Verification	<ul style="list-style-type: none"> <li>• Verifying malicious firmware update or modified firmware update on PC card cannot be installed on M100. (<a href="#">NY 7/12/07</a>) &amp; (<a href="#">CT 10/1/06 &amp; 7/1/07</a>) <ul style="list-style-type: none"> <li>• Verifying modified (malicious and non-malicious modifications) election definition of the file on PC card can not be installed.</li> <li>• Verifying the firmware version on M100.</li> <li>• Attempts to break into the M100 through the serial port fail.</li> <li>• Verifying no source code or compilers or assemblers are resident or accessible</li> <li>• Verifying locks can not be picked easily.</li> <li>• Attempt to insert the ballot prior to opening the polls. No votes can be recorded prior to opening the polls</li> <li>• Attempting to access the operating system on M100</li> <li>• Audit logs contain entries for failed attempts, normal &amp; abnormal events.</li> <li>• ENH18864 &amp; ENH18865 Artificial introduction of binary data errors in the memory</li> </ul> </li> </ul>

Method Detail	Security Test Method
	<p>devices transported between the HPM and scanning devices (M100 &amp; DS200) are reported, logged and handled by the scanning device prior to counting ballots.</p> <ul style="list-style-type: none"> <li>• Error logging modifications to the DS200 code base from the previously certified Unity 3.2.0.0 system tested through each branch of modified code.</li> <li>• DS200 reports the existence of a modem or absence of a modem in the audit log (tested further in the DS200 Functional Test Method).</li> </ul>
Pre-vote: Opening the Polls Verification	<ul style="list-style-type: none"> <li>• Verify zero totals report, to check vote count is "0" when the scanner is turned on.</li> <li>• Verify zero totals in memory and audit record of zero count.</li> </ul>
Voting: Ballot Activation and Casting Verifications	<ul style="list-style-type: none"> <li>• Attempt to remove the key, when the key is in voting mode.</li> <li>• Attempt to Insert blank ballot or invalid ballot (ballot from wrong election).</li> <li>• Attempt to scan multiple ballots.</li> <li>• Attempt to count the same ballot twice by physical manipulation</li> <li>• Attempt to print audit log as voter.</li> <li>• Attempt to remove the PC card in middle of the operation.</li> <li>• Attempt to unplug the power (without battery) to test recovery is possible.</li> <li>• Verify PC card insertion and removal is logged before closing the polls.</li> <li>• Audit logs contain entries for failed attempts, normal &amp; abnormal events.</li> <li>• Audit log cannot be printed during the voting mode</li> <li>• Remove paper source from the M100 to verify M100 election process halts.</li> <li>• Attempt to consolidate the PC card with open polls in ERM</li> <li>• Verify that the M100 when the PCMCIA card is write-locked refuses to scan ballots (NY 7/12/07)</li> <li>• BUG19853 When the audit log is full the DS200 will not allow any further scanning.</li> </ul>
Voting: Voting System Integrity, System Audit, Errors & Status Indicators	<ul style="list-style-type: none"> <li>• Audit logs contain entries for failed attempts, normal &amp; abnormal events.</li> </ul>
Post-vote: Closing the Polls	<ul style="list-style-type: none"> <li>• Attempt to reopen polls with invalid password</li> <li>• Verify key and 3 digit pin is required to reopen polls</li> <li>• Unable to modify the M100 audit log externally on the PC card validated through the M100 and ERM interfaces</li> <li>• Verify physical removal of internal modem</li> <li>• Unable to modify the M100 audit log through the system.</li> <li>• Unable to modem results through a modem connected to the serial port.</li> <li>• M100 serial port does not respond to 2 character queries or demonstrate that it is actively listening for commands</li> <li>• Modem attached to M100 serial port does not answer phone and generate a carrier signal.</li> </ul>
Post-vote: Central Count	<ul style="list-style-type: none"> <li>• Any direct, voting-application coordinated modification of vote counts requires authentication and username is logged.</li> <li>• Through the M100 interface, unable to manually modify vote counts.</li> <li>• If access to incomplete election results in ERM is present, the usage of it is configurable, but only by election administrators.</li> <li>• Any access to incomplete election results cannot modify any official results</li> <li>• Artificial introduction of binary errors in the memory devices transported between the scanning devices (M100 &amp; DS200) and the ERM are reported, logged and handled prior to consolidation.</li> </ul>
Post-vote: Security	<ul style="list-style-type: none"> <li>• Removing M100 PC card during consolidation at the ERM does not cause irreversible loss of data</li> <li>• Unplugging network cables during vote counting does not irreversibly affect these operations</li> <li>• Attempt to consolidate same PC card twice into ERM (KV•76 NY 7/12/07)</li> <li>• Verify that both slightly modified (non- malicious) election results and maliciously modified election results of the file on PC card from the M100 can not be loaded into ERM. (NY 7/12/07) &amp; (CT 10/1/06 &amp; 7/1/07)</li> <li>• Verify that the integrity of each data block of the DS200 and M100 results memory device is validated prior to being consolidated in ERM.</li> <li>• Verify that fuzzed election results of the file on PC card from the M100 can not be loaded into ERM. (KV•88, NY 7/12/07)</li> <li>• A guest user or an anonymous user is not allowed access to voting software or data files in ERM.</li> <li>• For networked system, different non- administrative users cannot access critical system files over the network and make undetected modifications to their content.</li> <li>• Manually input votes and verify authentication. (KV•84 NY 7/12/07)</li> </ul>

Method Detail	Security Test Method
	<ul style="list-style-type: none"> <li>• Attempt to log into the reporting ERM system and modify votes.</li> <li>• Audit logs contain entries for failed attempts, normal &amp; abnormal events.</li> <li>• Verify that access to incomplete election returns is configurable (If available) by an election administrator.</li> <li>• Verify that access to incomplete election returns provides no write-back access to the election return data.</li> <li>• DS200 diagnostic logs exist to enhance the vendor's ability to assess (post-mortem) non-recoverable errors, should they occur during an election cycle.</li> </ul>
Post-vote: System Audit	<p>Audit logs contain entries for failed attempts, normal &amp; abnormal events, pre-vote zero counts and failed pre-vote zero count tests.</p> <ul style="list-style-type: none"> <li>• BUG19664 errors are logged to the audit log.</li> <li>• In case the DS200 audit log is full, the audit log full event is recorded as well as the event leading up to the full event (i.e no events are lost)</li> </ul>
Additional Security	<p>See System Level and Telephony and Cryptographic Test Cases.</p> <p>Security Review Criteria:</p> <ul style="list-style-type: none"> <li>• Accept meets the guideline</li> <li>• Reject does not meet the guideline</li> <li>• NA the guideline does not apply</li> </ul>
Expected Results are observed	<p>All inputs, outputs, observations, deviations and any other information impacting the integrity of the test results will be recorded in the System Level and Security Test Case.</p> <p>A statement will be prepared addressing the results from the security perspective. It will provide the results of the testing and review required in vol. 1 section 6 for insertion in the test report</p>
Record observations and all input/outputs for each election;	Security Review and Test Case

#### 7.4.4 Telephony and Cryptographic Review and Testing

Testing was conducted on the system configuration identified in the PCA Configuration and Test Case.

Date	Test Result	Issues Opened	Issues Closed	Notes
4/14/2010	Accept			No connection to public networks

Method Detail		Telephony & Cryptographic Test Method
Test Case Name		Telephony and Cryptographic Test Case
Scope - identifies the type of test		Telephony and Cryptographic testing covers the use of public and non-physically controlled communications as well as the use of required cryptographic techniques in those subsystems for systems that use the public communications networks.
Test Objective		The Unity 3.2.1.0 voting system is exempt from the telecommunications and cryptographic requirements
Test Variables:		In the security review and security test case, the applicability of telephony and cryptography is assessed and tested. Confirm no telephony or non-local communications are utilized in the Unity 3.2.1.0 certification and therefore no telephony and cryptography test is required.
A description of the voting system type and the operational environment		The operational environment excludes any telecommunications and excludes any connection to public communications networks.
VSS 2002 vol. 1	5.1 thru 5.2.7, 6.5.3, 6.6.1	
VSS 2002 vol. 2	6.4.2	
Hardware, Software voting system configuration and test location	Not applicable	
Pre-requisites and preparation for execution of the test case.	During Pre-test Maintenance of the M100 observe that the M100 contains no modem or wireless transmitter.	
Getting Started Checks	Not applicable	
Documentation of Test Data & Test Results	Record observation of the absence of a modem or wireless transmitter in the M100.	
Pre-vote: Ballot Preparation procedures verifications	Not applicable	
Pre-vote: Ballot Preparation Security	Not applicable	
Readiness Testing and Poll Verification	Not applicable	
Pre-vote: Opening the Polls Verification	Not applicable	
Voting: Ballot Activation and Casting Verifications	Not applicable	
Voting: Voting System Integrity, System Audit, Errors & Status Indicators	Not applicable	
Post - vote: Closing the Polls	Not applicable	
Post - vote: Central Count	Not applicable	
Post - vote: Security	Not applicable	
Post - vote: System Audit	Not applicable	
Additional Security	Not applicable	
Expected Results are observed	Telephony and Cryptographic Test Cases. • NA the guideline does not apply	
Record observations and all input/outputs for each election;	Record observation of the removal or absence of the modem or wireless transmitter from the M100.	

#### 7.4.5 FCA Hardware Environmental Testing and reuse

Assessment and testing was completed on the hardware configuration identified [section 3.2 Voting System Test Environment](#). Assessment descriptions of the engineering changes submitted in Unity 3.2.1.0 are found [Table 1](#).

Date	Test Result	Issues Opened	Issues Closed	Notes M650 & AutoMARK VAT
9/18/2009	Accept			<b>M650 &amp; AutoMARK VAT - Unchanged-</b> - Assessment for reuse of the operating and non-operating testing in <b>ESSUNITY3200</b>
Date	Test Result	Issues Opened	Issues Closed	Notes - DS200 & Ballot Boxes
11/19/2009	Accept			<b>Assessment of ECO 000332:</b> <ul style="list-style-type: none"> <li><b>Non-operating Tests:</b> Change has no impact on transportation or storage. Reuse <b>ESSUNITY3200</b>.</li> <li><b>Operating Tests:</b> Change warrants repeating 4.8.3 VSS Electrostatic Disruption EN-61000-4-2</li> </ul>
11/19/2009	Accept			<b>Assessment of ECO 000339:</b> <ul style="list-style-type: none"> <li><b>Non-operating Tests:</b> Change has no impact on transportation or storage. Reuse <b>ESSUNITY3200</b>.</li> <li><b>Operating Tests:</b> Change has no impact on Operating- EMC. Reuse <b>ESSUNITY3200</b>.</li> </ul>
11/19/2009	Accept			<b>Assessment of ECO 000359:</b> <ul style="list-style-type: none"> <li><b>Non-operating Tests:</b> Change has no impact on transportation or storage. Reuse <b>ESSUNITY3200</b>.</li> <li><b>Operating Tests:</b> : Change warrants repeating 4.8.3 VSS Electrostatic Disruption EN-61000-4-2</li> </ul>
11/20/2009	Accept			<b>Assessment of ECO 000529:</b> <ul style="list-style-type: none"> <li><b>Non-operating Tests:</b> Change has no impact on transportation or storage. Reuse <b>ESSUNITY3200</b>.</li> <li><b>Operating Tests:</b> Change has no impact on Operating- EMC. Reuse <b>ESSUNITY3200</b>.</li> </ul>
11/11/2009	Accept			<b>Assessment of ECO 000843:</b> <ul style="list-style-type: none"> <li><b>Non-operating Tests:</b> Change has no impact on transportation or storage. Reuse <b>ESSUNITY3200</b>.</li> <li><b>Operating Tests:</b> : Change warrants repeating all EMC tests &amp; 4.1.2.6 VVSG Electrical Fast Trans EN-61000-4-4.</li> </ul>
11/20/2009	Accept			<b>Assessment of ECO 000841:</b> <ul style="list-style-type: none"> <li><b>Non-operating Tests:</b> Change has no impact on transportation or storage. Reuse <b>ESSUNITY3200</b>.</li> <li><b>Operating Tests:</b> : Change warrants repeating all EMC test except 4.8.8 VSS Magnetic Fields Immunity EN-61000-4-8 &amp; 4.1.2.6 VVSG Electrical Fast Trans EN-61000-4-4.</li> </ul>
11/20/2009	Accept			<b>Assessment of ECO 000844:</b> <ul style="list-style-type: none"> <li><b>Non-operating Tests:</b> Change has no impact on transportation or storage. Reuse <b>ESSUNITY3200</b>.</li> <li><b>Operation Tests:</b> : Change warrants repeating 4.8.3 VSS Electrostatic Disruption EN-61000-4-2</li> </ul>
11/20/2009	Accept			<b>Assessment of ECO 000847:</b> <ul style="list-style-type: none"> <li><b>Non-operating Tests:</b> Change has no impact on transportation or storage. Reuse <b>ESSUNITY3200</b>.</li> <li><b>Operating Tests:</b> : Change warrants repeating all EMC tests &amp; 4.1.2.6 VVSG Electrical Fast Trans EN-61000-4-4.</li> </ul>
1/26/2010	Accept			<b>Assessment of ECO 000534:</b> <ul style="list-style-type: none"> <li><b>Non-operating Tests:</b> Change has no impact on transportation or storage. Reuse <b>ESSUNITY3200</b>.</li> <li><b>Non-operating Tests:</b> Change has no impact on Operating- EMC. Reuse <b>ESSUNITY3200</b>.</li> </ul>
1/25/2010	Accept			<b>Assessment of ECO 000535:</b> <ul style="list-style-type: none"> <li><b>Non-operating Tests:</b> Change has no impact on transportation or storage. Reuse <b>ESSUNITY3200</b>.</li> <li><b>Non-operating Tests:</b> Change has no impact on Operating- EMC. Reuse <b>ESSUNITY3200</b>.</li> </ul>

1/15/2010	Accept			<b>Assessment of ECO 000576:</b> • <b>Non-operating Tests:</b> Change has no impact on transportation or storage. Reuse <b>ESSUNITY3200</b> . <b>Non-operating Tests:</b> Change has no impact on Operating-EMC. Reuse <b>ESSUNITY3200</b> .
8/11/2009 - 5/11/2010	Accept			<b>Assessment of ECO 000315, 000337, 000342, 000366, 000375, 000423, 000466, 000523, 000545, 000554, 000562, 000566, 000570, 000582, 000618, 000628, 000665, 000669 000674, 836, 837, 838, 839, 845, 846, and 851</b> • <b>Non-operating Tests:</b> Change has no impact on transportation or storage. Reuse <b>ESSUNITY3200</b> . <b>Non-operating Tests:</b> Change has no impact on Operating-EMC. Reuse <b>ESSUNITY3200</b> .
12/15/2009	Accept			<b>4.8.1 VSS Power Disturbance EN-61000-4-11-</b> successfully executed for ECO#:841, 843, 847
12/11/2009	Accept			<b>4.8.2 VSS Electromagnet Radiated &amp; Conducted Emissions FCC Part15B</b> successfully executed for ECO#:841, 843, 847
12/11/2009	Accept			<b>4.8.3 VSS Electrostatic Disruption EN-61000-4-2</b> successfully executed for ECO#:332, 359, 841, 843, 844, 847
12/12/2009	Accept			<b>4.8.4 VSS Electromagnetic Susceptibility EN-61000-4-3</b> successfully executed for ECO#:841, 843, 847
12/16/2009	Accept			<b>4.8.6 VSS Lightening Surge EN-61000-4-5</b> successfully executed for ECO#:843, 841, 847
12/15/2009	Accept			<b>4.8.7 VSS Conducted RF Immunity EN-61000-4-6</b> successfully executed for ECO#:843, 841, 847
12/16/2009	Accept			<b>4.8.8 VSS Magnetic Fields Immunity EN-61000-4-8</b> successfully executed for ECO#:843, 847
03/25/2010	Accept			<b>4.1.2.6 VVSG Electrical Fast Trans EN-61000-4-4</b> successfully executed for ECO#:841, 843, 847
Date	Test Result	Issues Opened	Issues Closed	Notes - M100
8/4/2009	Reject	1, 2, 27, 28		<b>M100- Unchanged -</b> Verification that the reports submitted for reuse from SysTest Unity 4.0.0.0 testing include: review of reports to confirm failures resulting in ECO were documented and hardware passed the tests, and review of all M100 material to ensure all required information is present.
9/8/2009	Accept		28	<b>M100-</b> Received ECO 682, verified documentation of the mitigation.
9/24/2009	Accept		1,2	<b>M100-</b> 4.8.3 VSS Electrostatic Disruption EN-61000-4-2 successfully conducted as required by NOC 08-001.
3/4/2010	Accept		27	<b>M100-</b> Verified SysTest Letter 3/3/10 Re: Sun APT Test Report: 06-00329, M100 Wireless, Testing Completed: 6/6/06 - 6/26/06 documents pass/fail results and the VSS requirements associated with the testing.

Identified issues are found in the [Unity 3.2.1.0 PCA and FCA Discrepancy Report](#).

Method Detail	Environmental Test Method
Test Case Name	Environmental Test Case
Scope identifies the type of test	<p>Assessment and testing of the hardware of the Unity 3.2.1.0 voting system for reuse of prior testing from <b>ESSUNITY3200</b> and SysTest Unity 4.0.0.0 testing for unchanged hardware and submitted engineering changes (ECOs):</p> <p><b>M100-</b> Review documented results SysTest's subcontractor testing in compliance with the EAC approval letter <i>8-04-09 Ltr to ESS reuse of testing final</i>, for both the VSS 2002 hardware operating and non-operating environmental tests. Determine applicability of the Electrostatic Disruption (ESD) test in accordance with NOC 08-001.</p> <p><b>M650 &amp; AutoMARK VAT-</b> Assess if there are any hardware changes since the <b>ESSUNITY3200</b> certified base line to determine applicable reuse testing from <b>ESSUNITY3200</b>.</p> <p><b>DS200</b> Identify and assess hardware changes from the <b>ESSUNITY3200</b> certified baseline and engineering change orders to determine applicable reuse testing from <b>ESSUNITY3200</b> testing and/or the extent of testing required, including execution and the provision of test results as</p>

Method Detail	Environmental Test Method
	<p>required.</p> <p>This set of hardware environmental test cases is outside the scope of iBeta's VSTL accreditation. Electrical testing was performed by Criterion Laboratories NVLAP #100396-0 (Electrical) with supervision of testing by iBeta. iBeta reviews and documents test records, results and reports to confirm testing was performed under an appropriate mode as a voting system and to determine acceptance or rejection of some or all testing.</p>
Test Objective	<p>Validation of the Unity 3.2.1.0 hardware to meet the Non-Operating/Operating Environmental test standards of the EAC VSS 2002, including:</p> <p><b>M100</b> Examination of the SysTest's subcontractor Non-Operating/Operating Environmental testing of the Unity 4.0.0.0 hardware to the EAC VSS 2002 for documentation of :</p> <ul style="list-style-type: none"> <li>• The tested hardware configuration;</li> <li>• A passing test results for the applicable requirements; and</li> <li>• Any engineering changes resulting from testing.</li> </ul> <p>Execution of the ESD test in accordance with NOC 08-001</p> <p><b>M650 &amp; AutoMARK VAT</b>-Verify no hardware changes have been made since EAC certification of <b>ESSUNITY3200</b></p> <p><b>DS200</b>Assessment of the ECOs from the <b>ESSUNITY3200</b> certified baseline to verify reuse of the Non-Operating Transportation and Storage test results from <b>ESSUNITY3200</b> and test execution of the Operating Electrical tests.</p>
Test Variables: Voting Variations (as supported by the voting system)	<p><b>DS200 - ECOs from the ESSUNITY3200 Criterion report issued for Unity 3.2.1.0</b></p> <p><b>M100 - Criterion ESD report issued for Unity 3.2.1.0 required by NOC 08-001</b></p> <p><b>M100 - Reuse of Unity 4.0.0.0 by EAC letter 8-04-09 Ltr to ESS reuse of testing final</b></p> <p><b>M650 &amp; AutoMark VAT - reuse of the certified baseline in the ESSUNITY3200 Test Report</b></p> <ul style="list-style-type: none"> <li>• Power disturbance disruption IEC 61000-4-11 (1994-06).</li> <li>• Electromagnetic radiation FCC Part 15 Class B requirements ANSI C63.4.</li> <li>• Electrostatic disruption IEC 61000-4-2 (1995-01).</li> <li>• Electromagnetic susceptibility IEC 61000-4-3 (1996).</li> <li>• Electrical fast transient protection IEC 61000-4-4 (1995-01).</li> <li>• Lightning surge protection IEC 61000-4-5 (1995-02).</li> <li>• RF immunity IEC 61000-4-6 (1996-04).</li> <li>• AC magnetic fields RF immunity IEC 61000-4-8 (1993-06).</li> </ul> <p><b>M100 - Reuse of Unity 4.0.0.0 by EAC letter 8-04-09 Ltr to ESS reuse of testing final</b></p> <p><b>DS200, M650 &amp; AutoMark VAT reuse of the certified baseline in the ESSUNITY3200 Test Report</b></p> <p><b>MIL-STD810-D:</b></p> <ul style="list-style-type: none"> <li>• High temperature method 501.2 Procedures I-Storage maximum 140 F degrees</li> <li>• Low temperature method 502.2, Procedure I-Storage minimum -4 F degrees</li> <li>• Temperature &amp; power variations method 501.2 &amp; 502.2</li> <li>• Humidity method 507.2</li> <li>• Vibration method 514.3-1 Category 1 Basic Transportation Common Carrier</li> <li>• Bench handling method 516.3 procedure VI</li> <li>• Safety OSHA CFR Title 29, part 1910</li> </ul>
A description of the voting system type and the operational environment	<p>Precinct Count scanner/tabulator: Model 100 (M100)</p> <p>Precinct Count scanner/tabulator: Model 200 (DS200)</p> <p>Central Scanner: Model M650</p> <p>Ballot Marking Device: Model AutoMARK VAT</p>
VSS 2002 vol. 1	3.2.2 thru 3.2.2.14, 3.4.8
VSS 2002 vol. 2	4.6.1.5 thru 4.7.1 & 4.8 RFI 2008-01, 2008-05, 2008-06, 2008-09, 2008-10, NOC 08-001
VVSG 2005 vol. 1	4.3.8, 4.1.2 thru 4.1.2.14

Method Detail	Environmental Test Method
VVSG 2005 vol. 2	4.6.1.5 thru 4.7.1 & 4.8
Hardware, Software voting system configuration and test location	<p><b>M650 &amp; AutoMARK VAT</b> configuration and test location is found in Appendix D of <b>ESSUNITY3200</b> Test Report.</p> <p><b>M100</b> Configuration and test location is found in Appendix B of the Unity 3.2.1.0 Test Plan.</p> <p><b>DS200 Electrical Testing and M100 ESD Testing</b> Test Location: Criterion Labs, Rollinsville CO</p> <ul style="list-style-type: none"> <li>• iBeta provided Criterion with the environmental hardware test case outlining methods for preparation of their test plan; iBeta documented the configuration, test environment, lab accreditations, tester qualifications, and operational status check performance</li> <li>• iBeta personnel execute the operational status checks and operate the equipment as a voting system during the EMI/EMC test execution.</li> </ul>
Pre-requisites and preparation for execution of the test case.	<p><b>M100</b>Determination of reuse from the EAC Receipt of the Unity v.4.0.0.0 test reports and engineering assessments from SysTest.</p> <p><b>M650 &amp; AutoMARK VAT</b>-Identify any hardware changes to the <b>ESSUNITY3200</b> certified voting system</p> <p><b>DS200 Electrical Testing and M100 ESD Testing:</b> Complete the prerequisites;</p> <ul style="list-style-type: none"> <li>• Validation and documentation of the subcontractor test labs' NVLAP accreditation in the specific test method identified in the Test Variables</li> <li>• Record the testers &amp; date</li> <li>• System has been set up as identified in the user manual</li> <li>• Gather any necessary materials or manuals.</li> <li>• Ensure customization of the test case template is complete</li> <li>• The iBeta approved Operational Status Check script is provided that includes: <ul style="list-style-type: none"> <li>◦ Checking the operation of all buttons, switches and lights</li> <li>◦ Opening the polls &amp; running a zero totals report</li> <li>◦ Checking appropriate error conditions for correct prompts or responses. (Error conditions will depend upon the type of equipment being tested.)</li> <li>◦ Accessibility features are operational.</li> <li>◦ Power off and on with no loss of function.</li> <li>◦ Close the polls and print all reports. (Totals &amp; Audit Logs)</li> </ul> </li> </ul>
Getting Started Checks	<p><b>M100</b>, For reuse of prior testing, Identify the appropriate report for each tested piece of equipment ; create the <i>Environmental Hardware Test Report Matrix</i></p> <p><b>M650 &amp; AutoMARK VAT</b>- none</p> <p><b>DS200</b> Check the voting system to:</p> <ul style="list-style-type: none"> <li>• Verify the test environment and system configuration is documented in the PCA Configuration and matches the vendor described configuration.</li> <li>• Validate installation of the Trusted Build</li> <li>• Testers understand that no change shall occur to the test environment without documentation in the test record and the authorization of the project manager</li> <li>• Confirm the tester understands the recording requirements of the iBeta test case</li> <li>• Operational status check procedures are available and successfully run</li> <li>• An automated script to loop system operation for use during the EMC operational tests exercises all necessary functionality.</li> </ul>
Documentation of Test Data & Test Results	<p><b>M100</b> - For reuse of prior testing, trace the equipment configuration for the VSS 2002 Non-operating/Operating test requirement to the applicable SysTest's subcontractor report in the <i>Environmental Hardware Test Report Matrix</i></p> <p><b>M650 &amp; AutoMARK VAT</b>-document no changes to the certified <b>ESSUNITY3200</b> baseline and reuse of the <b>ESSUNITY3200</b> test report</p> <p><b>DS200 Electrical Testing and M100 ESD Testing:</b> Test Results:</p> <ul style="list-style-type: none"> <li>• Enter Accept/Reject on the Test Steps</li> <li>• In Comments enter any deviations, discrepancies, or notable observations</li> </ul>

Method Detail	Environmental Test Method
Standard Environmental Tests	<ul style="list-style-type: none"> <li>Log discrepancies on the Discrepancy Report and insert the number in the Comments</li> </ul> <p><b>M100</b> Test reports from SysTest include test results for all applicable Non-operating/operating environmental hardware VSS 2002 required tests</p> <p><b>M650 &amp; AutoMARK VAT</b>-reuse the <b>ESSUNITY3200</b> Test Report</p> <p><b>DS200 Electrical Testing and M100 ESD Testing:</b>Follow test method in the identified international standard</p>
Expected Results are observed	<p><b>M100</b> Environmental test reports, SysTest Lab hardware assessments and engineering change documents identify:</p> <ul style="list-style-type: none"> <li>Non-operating/operating environmental hardware VSS 2002 required tests with a passing result</li> <li>Configuration of the tested hardware</li> <li>Engineering changes addressing any hardware mitigations</li> </ul> <p><b>M650 &amp; AutoMARK VAT</b>-No changes to the hardware since <b>ESSUNITY3200</b> certified baseline.</p> <p><b>DS200 Electrical Testing and M100 ESD Testing:</b> Review the test result against the expected result:</p> <ul style="list-style-type: none"> <li>Pass: meets the requirements</li> <li>Fail: does not meet the requirements; document the failure in the comments and in the PCA/FCA Discrepancy Sheet</li> <li>Not Testable (NT): not testable; provide a reason in the comments</li> </ul>
Record observations and all input/outputs for each election;	<p><b>M100-</b> All examination results will be documented in the <i>Environmental Hardware Test Reports Matrix</i> (Appendix B)</p> <ul style="list-style-type: none"> <li>Missing documents or clarification requests will be reported to the manufacturer as Document Defects in the Unity 3.2.1.0 Discrepancy Report</li> <li>Delivery and verification of documents and clarifications will be noted in the Unity 3.2.1.0 Discrepancy Report</li> </ul> <p><b>M650 &amp; AutoMARK VAT</b>- Record reuse of the <b>ESSUNITY3200</b> Test Report.</p> <p><b>DS200 Electrical Testing and M100 ESD Testing:</b> All test results will be recorded in the test case</p> <p>Any failure against the requirements will mean the failure of the system and shall be reported as such.</p> <p>Failures will be reported to the vendor as Defect Issues in the Discrepancy Report</p> <p>The vendor shall have the opportunity to cure all discrepancies prior to issuance of the Certification Report</p> <p>If cures are submitted the applicable test will be rerun. Complete information about the rerun test will be preserved in the test case. The cure and results of the retest will be noted in the Discrepancy Report and submitted as an appendix of the Certification Report</p> <p>Operations which do not fail the requirements but could be deemed defects or inconsistent with standard software practices or election practices will be logged as Informational Issues on the Discrepancy Report. It is the vendor's option to address these issues. Open items will be identified in the report</p>

## 7.5 Appendix E- Discrepancy Report

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
1	08/04/09	C Coggins	Docu- ment Defect	Closed	M100 HW Report - Criterion 080424-1241 Section 1.3	The potentially reusable M100 ESD test report does not identify the equipment serial number.  Section 1.3 Equipment under test identifies the model but not the serial number of the unit that went through hardware testing.	v.2: 4.6.1.1 Equipment identification... shall be recorded.	SLM 10.28.09 -ES&S no longer needs to reuse M100 HW Report - Criterion 080424-1241 Section 1.3. ES&S officially withdrew ECO# 775, which caused ES&S to rerun the ESD testing on the M100. A new EMC report will be issued by Criterion for this testing.	11/4/09 Accept CEC The request to reuse the report was withdrawn and an ESD test was successfully conducted.
2	08/04/09	C Coggins	Docu- ment Defect	Closed	M100 HW Report - Criterion 080424-1241 & ECO 775 Change Evaluation	There is no clear connection between potentially reusable M100 ESD test report and documentation of mitigation conducted during testing.  ECO 775 Change Evaluation identifies a mitigation to the M100, however no failure nor validation resolution is documented in either the SysTest Discrepancy Report or the sub-contractor ESD Test Report. The ECO775 Change Evaluation identifies "changes were modeled in the M100 and allowed it to pass ESD testing on 5/2/2008".	v.1: 9.6.2.6.a The ITA shall evaluate data resulting from examinations and tests employing the following practices: If any malfunction ... is detected that would be classified as a relevant failure using the criteria in Vol.2, its occurrence ... shall be recorded for inclusion in the analysis of data obtained from the test... EAC NOC 07-005 it is the lead VSTL's responsibility to properly test the voting system and accurately report those tests to the EAC.	SLM 10.28.09 -ES&S no longer needs to reuse M100 HW Report - Criterion 080424-1241 Section 1.3. ES&S officially withdrew ECO #775, which caused ES&S to rerun the ESD testing on the M100. A new EMC report will be issued by Criterion for this testing.	11/4/09 Accept CEC The request to reuse the report was withdrawn and a new ESD test was successfully conducted.
3	08/05/07	S Eaton	Docu- ment Defect	Closed	Unity 4.0 Discrepancy Report 07/6/07 (SysTest)  ES&S M100 System Maintenance Manual, V 5.4, HW Ver. 1.3, May 17, 2007	<b>From SysTest Unity 4.0 Testing - Disc:</b>  6 ES&S M100 System Maintenance Manual does not describe how data output is initiated and controlled or how power is converted.	v.2: 2.9.1: f. The description shall include a concept of operations that fully describes such items as: How data output is initiated and controlled; g. The description shall include a concept of operations that fully describes such items as: How power is converted or conditioned;	10.17.08 - RDG M100 SMM v.6.1.3.0_10.17.2008  Added additional information in the Electrical Information and M100 Concept of Operations sections in Ch 1: Introduction.	8/07/09 - Accept SLE Verified in Ch 1 of the M100 SMM, v.5.4, HW v1.3 10/17/08, that the documentation now describes how the data output is initiated and power is converted.
4	08/05/	S Eaton	Docu-	Closed	Unity 4.0	<b>From SysTest Unity 4.0 Testing - Disc:</b>	v.2:2.8.5: g. Supports	10.17.2008 - SS - M100	8/07/09 - Accept - SLE

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
	07		ment Defect		Discrepancy Report 7/6/07 (Sestets)  ES&S M100 SOP	<b>26</b>  ES&S M100 System of operations document did not provide a schedule for the software installation.	successful ballot and program installation and control by election officials, provides a detailed work plan or other form of documentation providing a schedule and steps for the software and ballot installation, which includes a table outlining the key dates, events and deliverables	SOP, ABCR SOP, M650 SOP - Sample timeline added to Ch 1 of all files	Verified in the M100 SOP FW 10/17/08 that ES&S provided a sample timeline in Ch 1: General Timeline for Election Preparation.
5	08/07/07	S Eaton	Docu-ment Defect	Closed	Unity 4.0 Discrepancy Report 05/18/07 (SysTest)  ES&S M100 SOP FW Ver. 5.4.0.0, HW Rev. 1.3, February 29, 2008	<b>From SysTest Unity 4.0 Testing - Disc:</b>  <b>27</b>  ES&S M100 System of Operations does not provide procedures for product acquisition there is no reference to PDTR readiness testing documents, and does not provide information on system maintenance, correction of defects, and incorporating hardware and new software releases.  (Note: Ch 13: Combining M100 and iVotronic Results, Pre-election day setup heading, Test the PEB Setup subheading is out of scope of Unity 3.2.1.0. It will be testing in Unity 4.0 when the iVotronic is added.)  <b>8/7/09 Reject - SLE:</b> Ch 3: Understanding the Counter and Ch 7: Maintaining the Counter does not contain information on understanding or maintaining the counter.	v. 2: 2.8.6: a. Defines the procedures required to support system acquisition, installation, and readiness testing. These procedures may be provided by reference, if they are contained either in the system hardware specifications, or in other vendor documentation; b. Describes procedures for providing technical support, system maintenance and correction of defects, and for incorporating hardware upgrades and new software releases.	<b>MDN - 1.18.2010-</b> Updated document delivered with TDP Rev7 1.12.2010. Revisions described below.  <b>DJZ - 11.20.2009</b> - On 10-29-09 SOP Added a note to M100 SOP Ch 3, referring the reader to Ch 7 for maintenance procedures. Added a note to Ch 7 referring to Ch 3 for content describing the scanner.  <b>DJZ 10.29.2009</b> - Added a note to M100 SOP Ch 3, referring the reader to Ch 7 for maintenance procedures. Added a note to Ch 7 referring to Ch 3 for content describing the scanner.  <b>TMT-2/26/2008-M100 SOP - 2.8.6a for System Acquisition and Installation see Ch.3: Understanding the Counter, Ch.4: Performing Pre-Election Day Tasks. For Readiness Testing See Ch.4: Performing Pre-Election Day Tasks, the ""Checking the Election</b>	<b>Accept 1/29/10 KA Ch 3 &amp; Ch 7 cross references for understanding &amp; maintaining the counter. SOP 10/20/09</b>  <b>8/7/09 Accept -SLE</b> - Verified in M100 SOP FW 10/17/08  Operations Support FAQ addresses system purchased, installation, setup, training needed, and with a checklist; Product acquisition and PDTR readiness testing, is ad-dressed in Ch 1, 3, 6, 10, & 11. System maintenance, correction of defects, and incorporating HW and new SW releases, are addressed in Ch 1, 2, 4, 7, 9 & 12  <b>8/7/09 SLE Reject Ch 3 &amp; 7</b>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							<p><i>Definition for Accuracy</i>" and ""Testing the Election Definition"" headings, Ch.5: Performing Election Day Tasks, Ch.9: Understanding System Messages, and Ch.10: Understanding System Menus. Ch.13: Combining M100 and iVotronic Results, Pre-election day setup heading, Test the PEB Setup subheading.</p> <p>2.8.6b sees Ch.1: Introduction, Contacting ES&amp;S for Technical Support, Ch.2: Understanding Warning Symbols, Ch.7: Maintaining the Counter, Ch. 8: Understanding Reports, Ch. 11: Troubleshooting. Also for updating or upgrading information, refer to Ch.12: Loading New Firmware onto the M100. M100 SOP 8.22.08 - Ch. 1: Introduction Added System Acquisition Procedures section.</p> <p>10.17.2008 - M100 SOP - Ch.1: Overview, Added a new heading, Operations Support FAQs, providing information about: how the system is purchased, how the system is installed, setup of the system, how a user can verify the system the training needed, the checklist to be followed.</p>		

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
6	08/05/07	S Eaton	Document Defect	Closed	Unity 4.0 Discrepancy Report 01/16/08 (SysTest)  ES&S M100 SOP FW v.5.4.0.0, HW rev. 1.3 11/16/07	<b>From SysTest Unity 4.0 Testing - Disc: 372</b>  ES&S M100 System of Operations documents do not indicate how the scanners track or report on paper provisional ballots.	v.1:4.2: Consolidating Vote Data- All systems shall provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes).			89/5/09 Accept CEC Processing of provisional ballots is a manual procedure and not a function of the scanner
7	08/05/07	S Eaton	Functional Defect	Closed	Unity 4.0 Discrepancy Report 04/24/08 (SysTest)  Model 100 v. 5.4.0.0	<b>From SysTest Unity 4.0 Testing - Disc: 428</b>  M100 accepted fake ballots that were copied from un-voted original ballots on a laser color copier printer (XEROX WORKCENTRE 7665).  <b>02/18/10 Rejected JG KA</b> Using blank ES&S ballot stock, a Xerox Docucolored 250 laser color copied ballot was accepted by the M100.	v.1 : 6.1  Systems are: To protect the system from intentional manipulation and fraud, and from malicious mischief	<b>SLM - 03.19.10</b> - The M100 (firmware v. 5.4.4.0) does not support the counterfeit ballot mark and therefore will not be included in the release of Unity 3.2.1.0.  Physical security and manual control of all ballots and ballot stock by the election office is paramount to limit access to ballots and ballot stock before, during and after the election. ES&S' System Security Spec - Ch 3 - Managing Security covers these such practices  <b>SLM - 03.09.10</b> ES&S withdraws the previous statement of 10.27.09. There is no calibration setting on the M100 for counterfeit detection. ES&S addressed this issue in the new M100 firmware drop V. 5.4.4.0. Also, ES&S enhanced the counterfeit detection mark itself on the ballot stock. ES&S will be sending new ballots that have the enhanced	<b>3/19/10 Accept CEC</b>  VSSv.1: 6.1 identified by SysTest isn't a test requirement. It's a definition of Ch. 6 scope. Verified Ch. 3 - ESS Sec Spec identified physical security tracking and protection of ballots. A search of the documents listed below confirmed that there were no references to support of the counterfeit ballot detection on the ballot stock or references to counterfeit or photocopied ballots.  This issue was transferred from the Unity 4.0 SysTest test effort. iBeta has no knowledge of the circum-stances that lead to the original testing.  Docs reviewed: ES&S Sys Sec Spec Ver. Rel. 3.2.1.0 2/24/10, M100 SOP FW v. 5.4.4.0 HW rev.1.3 2/26/10;  ES&S Sys Func Descp, M100 Unity v. 3.2.1.0 3.9/10, & Voting Sys Over-view Unity v.3.2.1.0 rev.8 .0 2/26/10.	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								<p>counterfeit detection mark to be ran as part of the testing.</p> <p><b>ERW 10-27-2009</b> The M100 is equipped with a sensor that can detect the difference between an original ballot with a counterfeit mark printed in special ink or one that is copied. If the election definition calls for counterfeit detection and the sensor is properly calibrated this functionality works as documented.</p>	02/18/10 Reject JG KA
8	08/05/07	S Eaton	Document Defect	Closed	Unity 4.0 Discrepancy Report 09/24/08 (SysTest)  ES&S Sys Overview Ver. 4.0.0.0 August 22, 2008	<b>From SysTest Unity 4.0 Testing - Disc: 551</b>  ES&S M100 System Overview does not state that the scanner can be used as a central count scanner as stated in the M100 SOP, Ch 1.	v.2: 2.2.1.b  The system description shall include written descriptions, drawings and diagrams that present: A description of the operational environment of the system that provides an overview of the hardware, software, and communications structure	<b>MDN - 10.02.2008</b> - System Overview - Added a brief statement to Section 1.2.1 describing the Model 100's utility as a central scanner.	<b>8/07/09 Accept SLE - Verified in M100</b>  System Overview ver. 4.0.0.0 10/20/08 that ES&S addressed the issue by adding a statement regarding the M100's utility as a central scanner.
9	08/13/09	K Swift	Functional Defect	Closed	ERM v. 7.5.0.0 40HTEST1 TC	<b>Issue 35 transferred from Unity 3.2.0.0 From SysTest Unity 4.0 Testing - Disc: 475</b>  Numbered Key - Districts report is showing two M650 groups and the iVo PEB group does not appear; however, the PEB totals match the totals appearing alongside the second M650 group totals (it appears that the 'label' is incorrect and should read 'IVO PEB'). I then went into add/change groups and switched the location of the M650 group and the M100 group, regenerated the report and we now show two M100 groups and again the iVo totals appeared under the second M100 group. It seems the report is mimicking the name in group three into group four, but applying the correct totals. Copies of the report and screen shot of the add/change groups faxed to	v.1: 4.4.4.a, b  Voting systems shall meet these reporting requirements by providing software capable of obtaining data concerning various aspects of vote counting and producing reports of them on a printer. At a minimum, vote tally data shall include:  a. Number of ballots cast, using each ballot configuration, by tabulator, by precinct, and by political subdivision; b. Candidate and measure vote totals for each contest, by tabulator;	<b>Sue - 10.02.08</b> - This issue will be resolved in the latest software drop of ERM 7.5.2.0.  <b>Sue - 04.03.09</b> - Please review using updated software.  <b>Sue - 05.19.09</b> - The scope of Unity 3.2.0.0 does not contain the number (3) of groups to test this.	<b>04/01/10 SE &amp; JG Accept – Verified in ERM v. 7.5.6.0 that the Numbered Key - District Only report displays the groups correctly. After creating the groups and reading in results, we changed the groups again and verified that they displayed correctly in the same report. See #144 – this was opened because results did not display with the correct groups.</b>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
10	08/13/09	S Sivixay	Document Defect	Closed	ES&S System Limitations Unity v. 3.2.1.0 3/11/09	<p>vendor.</p> <p>There are two different ERM limitation displayed for a single characteristic.</p> <p>In Section 2.2 (Model 100) of the Limitations document it states the Maximum candidate counters allowed per precinct is 1020 however, in section 2.1 (DS200) the Maximum candidate counters allowed per precinct is displayed as 1000. The limitation is an ERM limitation and not a hardware (DS200, M100) limitation.</p>	v.2: 2.3 <i>The vendor shall provide a listing of the system's functional processing capabilities, encompassing capabilities required by the Standards and any additional capabilities provided by the system such as candidate counters per precinct</i>	<b>MDN 09.02.09.</b> Updated Section 2.2. of the limitations document to reflect ERM system limitations (Document rev4)	<b>09/16/09 Accept - SLE</b> Verified the ERM limitations were corrected in Section 2.2.
11	08/13/09	S Sivixay	Document Defect	Closed	ES&S System Limitations Unity v. 3.2.1.0 3/11/09	<p>Inconsistencies on the M100 maximum contests per election</p> <p>In Section 2.2.1 (Model 100) of the Limitations document it states the M100 supports a maximum of 255 contest per ballot style but, Section 2.2 states the maximum contests allowed per ballot style is 250 or # of positions on ballot.</p>	v.2: 2.3 <i>The vendor shall provide a listing of the system's functional processing capabilities, encompassing capabilities required by the Standards and any additional capabilities provided by the system such as maximum # of contest per a single ballot style</i>	<b>MDN 09.02.09.</b> Updated the maximum supported contests per ballot style for the Model 100 in sections 2.2 and 2.2.1 to 200 based on internal testing (Document rev4).	<b>09/16/09 Accept - SLE</b> Verified Sect 2.2 and 2.2.1 consistently state that the M100 supports a maximum of 200 contests per ballot style.
12	08/13/09	M Warner	Document Defect	Closed	ES&S M100 System Ops Procedures FW v.5.4.0.0 HW Rev 1.3 3/11/09	<p>Does not describe steps needed to prepare (format) the PCMCIA card</p> <p>Model 100 elections are programmed in accordance with the ballot requirements of the election and stored on the PCMCIA SRAM card, but the M100 system operating procedures do not describe the steps needed to prepare the PCMCIA card.</p>	v.2: 2.8.5.g <i>The vendor shall provide documentation of system operating procedures that meets the following requirements: To support successful ballot and program installation and control by election officials, provide a detailed work plan or other form of documentation providing a schedule and steps for the software and ballot installation, which includes a table outlining the key dates, events and deliverables;</i>	<b>DJZ - 8-28-09 - M100 SOP</b> - Added note to page Ch 3: Description of Model 100, PC Card on pg 12. The PCMCIA card does not require it to be formatted. The card uses a block memory device and does not have to be formatted or erased as it is overlaid with a block of data with a defined length. You will need ES&S proprietary software and hardware to write, modify and read the PCMCIA card. - HPM is used to write the election definition onto the PCMCIA card. - The M100 reads the election definition from the PCMCIA card,	<b>09/15/09 Accept SLE - ES&amp;S Model 100 System Operations Procedures Firmware Version 5.4.0.0 Hardware revision 1.3</b> 8/28/09 provides a note stating that the PCMCIA card does not require formatting

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								modifies the results and status area as ballots are tabulated and writes log entries as appropriate. - ERM is used to read the results from the PCMCIA card	
13	08/14/09	M Warner	Document Defect	Closed	ES&S SW Design Spec Model 100 Unity v. 3.2.1.0 8/11/09	<p>HARDWARE ENVIRONMENT AND CONSTRAINTS section mentions DS200, not M100</p> <p>In the "ES&amp;S Software Design Spec Model 100" manual, in the Hardware Environment &amp; Constraints table, the "Peripheral Device Interface Hardware" hardware characteristic description says "PCMCIA SRAM card are the devices interfacing with the DS200", but doesn't mention the M100.</p>	v.2.2.5.5.1.d Hardware Environment and Constraints - The vendor shall identify and describe the hardware characteristics that influence the design of the software, such as: d.) Peripheral device interface hardware;	<b>MDN 09.02.09.</b> Corrected in document Revision 4 (TDP Rev3). Information was correct. Referenced tabulator was incorrect.	<b>09/15/09 Accept - SLE</b> Verified in the ES&S SW Design Spec Model 100 Unity v.3.2.1.0 Rev 4.0 that the DS200 tabulator reference was changed to M100.
14	08/17/09	M Warner	Document Defect	Closed	ES&S System HW Spec Model 100 Unity v. 3.2.1.0 8/11/09	<p>ELECTROMAGNETIC ENVIRONMENT section mentions DS200, not M100</p> <p>In the ES&amp;S System Hardware Specification Model 100 manual, the ELECTROMAGNETIC ENVIRONMENT section refers to the DS200, but does not mention the M100.</p>	v.2.2.4.2.b The vendor shall provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for qualification testing. The vendor shall provide a list of materials and components used in the system and a description of their assembly into major system components and the system as a whole. Paragraphs and diagrams shall be provided that describe: b.) The electromagnetic environment generated by the system	<b>MDN 09.02.09.</b> Corrected in document Revision 4. Replaced references to the DS200 in Sections 2.1.8, 2.3.4.1, 2.3.5 and 2.4 with Model 100 references. Device name was not updated within ES&S boilerplate content.	<b>09/15/09 Accept - SLE</b> Verified in the ES&S System HW Spec Model 100 Unity v. 3.2.1.0 Rev 4 that the M100 replaced the DS200 in sect.2.4 Electromagnetic Environment, as well as sections 2.1.8, 2.3.4.1 and 2.3.5
15	08/18/09	Sjakileti	Document Defect	Closed	ES&S System Security Spec Ver. Rel. 4.0.0.0 8/27/09	<p>The System Security Specification does not address the security changes submitted as part of Unity 3.2.1.0.</p> <p>We have not received a System Security Specification updated for Unity 3.2.1.0. The delivered specification indicates that</p>	v.2: 2.1.1.1f : Required Content for Initial qualification At minimum, the TDP shall contain the following documentation f: System security specifications	<b>MDN 09.02.09.</b> Security specification disclaimer updated to reflect support for the model 100 and an EMS file server. Specifications versioning also updated	<b>10/12/09 Accept SJ:</b> Verified ES&S System Security Spec Ver. Rel. 3.2.1.0 9/25/09 was updated with M100 information

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p><i>the M100 is excluded.</i></p> <p><b>09/16/09 SLE Reject -</b> While the M100 exclusion was fixed in the disclaimer, the document does not contain any security specifications for the M100.</p> <p>Specifications for the M650 and DS200 are identified, but there is no information for the M100.</p>		<i>to reflect the system version (Unity 3210).</i>	<b>09/16/09 SLE Reject</b>
16	08/18/09	K. Wilson	Document Defect	Closed	Voting System Overview Unity v. 3.2.1.0 Rev 6.0 12/30/09	<p>The System Overview does not clearly identify the operation of the local EMS network, and file specifications</p> <p>Sect. 1.4 contains a diagram of the Election Definition File Server however no corresponding entry for a subcomponent appears in sect. 1.5 and no interfaces for the device appear in sect. 1.6. Existence of a "file server" suggests that some files are shared between workstations and these files are not defined as a part of the interfaces specification section. It is not clear whether the network is introduced simply to facilitate work flow or whether actual files or databases are being shared simultaneously by workers at each workstation.</p> <p><b>10/26/09 KGW Reject --</b></p> <p>a) Fig1.4.1 stand-alone: The diagram doesn't reflect 1 stand-alone PC attached to a printer which performs Election Definition, Equip Prep, Results Consolidation &amp; Reporting functions. The diagram reflects 4 PCs, a network hub and Electionware SW</p> <p>b) Fig1.4.2 Peer to Peer: "Election Coding Center- Closed Network" shows a server. Multiple EMS PCs reflect the same SW applications and not the separate election definition and central count configurations submitted (i.e. 1 PC with EDM, ESSIM, HPM, AM, &amp; AIMS; 1 or more PCs with ERM). In the submitted configuration 1 separate AIMS PC could reside on the network if AIMS isn't installed on the other election</p>	<p>v.2:2.2.1 c. A theory of operation that explains each system function, and how the function is achieved in the design; ... e. Identification of ... communications services used in the development and/or operation of the voting system, identifying the name, vendor and version used for each such component, including ...f. Interfaces among internal components, and interfaces with external systems. For components that interface with other components for which multiple products may be used, the TDP shall provide an identification of:</p> <p>1) File specifications, data objects, or other means used for information exchange;</p>	<p><b>MDN - 1.18.2009 - Updated document delivered with TDP Rev7 1.12.2010. See Sections 1.2.1, 1.4 and 1.7</b></p> <p><b>MDN 10.16.09._System Overview - -Updated diagrams in Section 1.4 of the Unity 3210 System Overview to detail the equipment configurations for all three system setups (standalone, peer-to-peer and Windows 2003 closed network.). Added both the peer-to-peer and Windows Server 2003 file server to the component list in Section 1.5. Added section 1.6.1.1 describing the interfaces included in a networked EMS.</b></p> <p><b>MDN 09.02.09._ES&amp;S is updating system drawings and descriptions. To be provided in a later documentation drop.</b></p>	<b>02/12/10 Accept KA &amp; KGW</b> Verified: Fig.1.4.1 reflects a stand alone PC, Fig. 1.4.2 no longer shows a server Fig 1.4.2 and Fig 1.4.3 show SW applications correctly configured to PCs, The concerns of v.1:6.5.6.b are addressed in another document.  <b>2/9/10 Reject KA &amp; KGW</b>  <b>10/25/09 Reject KGW</b>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						definition PC. c) Fig1.4.2 Peer to Peer: The "Results Consolidation and Reporting" networked "Results Display Workstation" doesn't address v.1:6.5.6.b regarding the limiting of interactive queries with no provision for write-access back to the system. d) Fig1.4.3 Window 2003 Server: Same comments as b) and c) apply except that inclusion of the Windows Server 2003 is correct.			
17	08/18/09	C Coggins	Docu-ment Defect	Closed	Requirements of the 2005 VVSG Trace to Vendor Testing and TDP 8/11/09	The location of the System Change Notes for Unity 3.2.1.0 was not identified. Unity 3.2.1.0 is a change to Unity 3.2.0.0. Submission of Change Notes was not identified (see v.2:2.13 a - d for the required content of the System Change Notes)	v.2: 2.13 Vendors submitting a system for testing that has been tested previously by the test authority and issued a qualification number shall submit system change notes.	MDN 09.02.09._System change notes Rev 1.0 added in TDP Revision 3. File name is U3210_OVR03_CngNts. Location is under the System Overview Sec. Document Identified in updated trace matrix delivered with TDP Rev3 delivered 20090903	<b>09/16/09 Accept - SLE</b> Verified the System Change Notes were delivered.
18	08/18/09	K. Wilson	Docu-ment Defect	Closed	Hardening Procedures for the Election Management System PC 8/11/09	<i>The Hardening Procedures are insufficiently detailed.</i>  <i>Ch 11 states "The following steps are provided as a means to migrate a PC previously hardened to the older ES&amp;S specifications to the newer specifications now contained in this document." It is unclear what "the older ES&amp;S specifications" are and if earlier scripts defined in the document have been revised. The document refers to 080407a.inf, registry.pol and secure.reg files. It is unclear if these files have changed or may change over time because there is no revision information provided. If these files have not changed then the documentation is unclear because Ch 11 must always be performed regardless of whether the earlier chapters are performed.</i>	v.2:2.4.2 The vendor shall provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for qualification testing.	<b>Brian B. 8/28/09 -- Ch 11 has been removed and the hardening document updated for clarity.</b>	<b>09/15/09 Accept - SLE</b> Verified that Ch 11 was removed from Hardening Procedures for the EMS PC 09/08/09.
19	08/19/09	S. Eaton	Docu-ment Defect	Closed	Requirements of the 2005 VVSG Trace to Vendor Testing and TDP 8/11/09	<i>The Unity 3.2.1.0 "Supported Functionality Declaration" was not provided.</i>	v.2: 2.2: In the system overview, the vendor shall provide information that enables the test authority	<b>MDN 09.02.09._Included with TDP Rev3 (Delivered 20090903).</b>	<b>09/15/09 Accept - SLE</b> Verified 2002 VSS Supported Functionality

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						The matrix of Unity 3.2.1.0 TDP documents identifies U3210_OVR01_SupportedFunctDec (Supported Functionality Declaration) as part of the System Overview documents. It was not submitted in the delivery of Unity 3.2.1.0 TDP.	to identify the functional and physical components of the system, how the components are structured, and the interfaces between them.		Declaration was delivered.
20	08/19/09	K. Swift	Functional Defect	Closed	ERM v. 7.5.2.0 Creating results database (TC v8s1)	<p><b>Issue 104 transferred from Unity 3.2.0.0</b></p> <p>In HPM when the System Type is set to the "Central Count" option in an election that is only using an M650 Central Scanner, an error is generated in ERM when creating results database.</p> <p>If the System Type is set to "Central Count" in HPM on an election with only an M650 (using the M650 limit of 3750 counters), opening the election in ERM will generate the error "Pgm Aero terminated with return code 253; Cobol error code 109" and shutdown ERM. On attempting to re-launch ERM the following messages display: "Convert Precinct Results File: The precincts results file is from older software and is being converted." and "Error: File: Vol8S1.CTR, Error: #35 - File does not exist." The election cannot proceed. If the System Type is reset to "Both" (i.e. a precinct and a central scanner) the election processes correctly. However the user is then required to complete the definition of a non-existence precinct scanner.</p> <p><b>4/20/09</b> iBeta requested further clarification of the not supported statement. Where is it supported? Is there a plan to fix the issue?</p>	v. 1: 2.2.6.d An EMS shall generate and maintain a database ...that enables election officials ...to perform the following functions: generate ballots and election-specific programs for vote recording and vote counting equipment; and h. generate the post voting reports required by section 2.5	<p><b>MDN 2009.10.30-</b> This issue is addressed with ERM v. 7.5.5.0.</p> <p><b>MDN 2009.06.16-SOP00_HPM Ch13</b> Updated with TDP revision 3 submitted 04.09.2009 based on internal review. Step 6 includes the instruction, "From the System Type list, select Both. This is the only equipment type being supported by ES&amp;S. NOTE: The Central Count, Precinct Count and Mixed system types are not supported."</p> <p><b>4/23/09 extract from email:</b> The 109 error during the ERM Database create process is the result of the implementation of the new bounds checker first implemented in Unity 4.0 / 3.2. When election type is set to 'Central' instructions intended for legacy tabulation equipment not being certified with this release are executed. When the election type is set to 'Both' in HPM, the ERM Database successfully executes intended instructions and stores</p>	<p><b>4/22/10 Accept JG</b> Tested and verified in ERM v. 7.5.6.0 when using any of the System Types "Both, Central Count, Precinct Count or Mixed Mode" ERM does not error when creating a results database.</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								<p>the certification message lines entered in HPM into the ERM Database. Using election type 'Both' in HPM vs. 'Central' doesn't affect processing in HPM for tabulation equipment certified in this release. The election type setting is only used to disable certain menu and screen options for precinct based equipment and does not affect any tabulator parameter files created in HPM or data used by ERM to create the database. This issue will be fixed in Unity 4.0.</p>	
21	08/18/09	M.Warner	Document Defect	Closed	System Overview Unity v. 3.2.1.0 3/11/09	<p>M100 absent from Table of Contents in System Overview document.</p> <p>The M100 is absent from Table of Contents, even though it appears as item 1.2.1 in the Operational Environment section.</p>	<p>v.2.2.1.1.3 The TDP shall include a detailed table of contents for the required documents, an abstract of each document and a listing of each of the informational sections and appendices presented.</p>	<p><b>MDN 2009.09.25-OVR00 Rev4</b> -- updated the table of contents to include Model 100 document sections</p>	<p><b>Accept 10/12/09 SJ:</b> Verified System Overview Unity v.3.2.1.0 9/28/09 includes M100 in table of contents</p>
22	08/18/09	M.Warner	Document Defect	Closed	System Overview Unity v. 3.2.1.0 3/11/09	<p>M100 absent from System Description in System Overview document.</p> <p>The M100 is absent from the chart in the System Description section, even though it appears as item 1.2.1 in the Operational Environment section.</p>	<p>v.2.2.2.1.b The system description shall include written descriptions, drawings and diagrams that present: b. A description of the operational environment of the system that provides an overview of the hardware, software, and communications structure;</p>	<p><b>MDN 2009.09.25-OVR00 Rev4</b> -- updated the system description table under Section 1 with versioning for the Model 100</p>	<p><b>Accept 10/12/09 SJ :</b> Verified System Overview Unity v.3.2.1.0 9/28/09 includes the M100 in the system description table</p>
23	08/20/09	Sjakileti	Document Defect	Closed	System Functionality Description Model 100 Unity v.3.2.1.0 v.3.0	<p>System description is inconsistent.</p> <p>M100 is submitted for testing as a precinct count system, but documentation identifies the M100 as a paper-based, central count system. (Section 1.1.2. f, 1.1.4, DRE System</p>	<p>v.1:9.2 The vendor shall submit to the ITA documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of</p>	<p><b>MDN 2009.09.25-SFD00_M100 Rev4</b> -- Referenced sections included boilerplate verbiage indicating non-support of DRE requirements. These</p>	<p><b>Accept 10/12/09 SJ:</b> Verified ES&amp;S SFD Model 100 Unity v.3.2.1.0 9/28/09 does not reference the M100 as a central tabulator</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						Requirements, 1.3.3.3 e-z)	an appropriate test plan by the ITA for system qualification testing.	sections have been revised to remove the central tabulator reference.	
24	08/21/09	S. Eaton	Document Defect	Closed	Model 100 System Operations Procedures FW HW revision 1.3 3/11/09	<p>System limit identified in the SOP does not match the System Limits documentation.</p> <p>The "Enable Multiple Precincts for Testing" section of the SOP is not consistent with the system limitations document. The SOP states that the Model 100 can process ballots for up to 10 precincts for Election Day voting, while the System Limitations states that the maximum precincts allowed in an election is 18.</p>	v.2.2.8 This documentation shall provide all information necessary for system use by all personnel who support pre-election and election preparation, polling place activities and central count activities, as applicable, with regard to all system functions and operations....	<b>DJZ - 9-18-09 - M100 SOP - Ch 5: Enable Multiple Precincts For Testing; pg 32.</b> Updated number of precincts allowed.	<b>Accept 10/12/09 SJ:</b> Verified ES&S Model 100 SOP FW v.5.4.0.0 HW rev. 1.3 identifies M100 can process ballots for up to 18 precincts for election day voting
25	08/24/09	Sjakileti	Document Defect	Closed	System Functionality Description Model 100 Unity v. 3.2.1.0 3/11/09	<p>In the security document review no mention was found regarding access to incomplete election returns and interactive queries</p> <p><b>Rejected 10/1/09 SJ:</b> This requirement applies as well to polling place equipment that contains a removable memory module, or that may be removed in its entirety to a central place for the consolidation of polling place returns.</p>	v.1: 6.5.6 Access to Incomplete Election Returns and Interactive Queries -If the voting system provides access to incomplete election returns and interactive inquires before the completion of the official count, they system shall: For equipment that operates in a central counting environment, be designed to provided external access to incomplete election returns only if that access for these purposes is authorized by the statutes and regulations of the using agency. This requirement applies as well to poling place equipment that contains a removable memory module, or that may be removed in its entirety to a central place for the consolidation of polling place returns.	<b>MDN 2009.10.16-SFD00_M100 Rev4 --</b> Added Section 1.1.5.2 to the Model 100 SFD addressing access controls on incomplete election results.  <b>MDN 2009.09.25-SFD00_M100 Rev4 --</b> This requirement relates to network results transmission over standard telecommunications lines (polls to election central results transmission), which is not supported in Unity 3.2.1.0.	<b>Accept 10/23/09 SJ:</b> Verified SFD Model 100 Unity v.3.2.1.0 10/20/09 addresses access to incomplete election returns  <b>Reject 10/1/09 SJ</b>
26	08/24/	Sjakileti	Docu-	Closed	Model 100	There are no security procedures	v.1:6.3.2 Vendors shall	<b>MDN 2009.09.25-</b>	<b>Accept: 9/30/09 SJ:</b>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
09			ment Defect		System Ops Procedures FW HW rev 1.3 3/11/09	<p>identified for using the M100 as a central count scanner.</p> <p>It is stated that the M100 can be used as central count system, but procedures do not specify what physical and procedural security controls are required in the central count location</p>	<p>develop and document in detailed measures to be taken in a central counting environment. These measures shall include physical and procedural controls related to the Handling of ballot boxes Preparing of ballots for counting Counting operations and Reporting data</p>	OVR00 Rev4 -- • Updated Section 1.2.1 "Using the Model 100 as a Central Ballot Tabulator" to apply recommended procedures from the ES&S System Security Specifications for central count equipment to a Model 100 central count environment. Updated Ch 5 of the System Security Specification (SSS00) to detail security requirements by environment.	Verified update of central count security procedures in System Sec Spec 9/25/09
27	08/31/09	C Coggins	Docu-ment Defect	Closed	ES&S Retest Matrix v.1.16 - M100 testing (SysTest)  Sun Micro-systems APT Test Service Report APT Job # 06-00329 (Final Approval 7/21/06)	<p>Potentially reusable Unity 4.0 hardware test results do not identify whether the M100 passed or failed. Neither does it identify the VSS nor corresponding international test standard.</p> <p>The matrix indicates the APT report contains the results of M100 testing on pg 3. The report does not provide pass/fail results. The report lists an order of tests but these tests do not identify either the VSS or international standard corresponding to the identified test.</p>	v.2: B.5 The test report shall be organized so as to facilitate the presentation of conclusions ...a summary of test results ...	SLM 10.29.09 - ES&S is working with SysTest Labs and Sun to resolve this issue.	Accept 3/4/10 - CEC - SysTest Letter 3/3/10 Re: Sun APT Test Report: 06-00329, M100 Wireless, Testing Completed: 6/6/06 - 6/26/06 documents pass/ fail results and the VSS requirements associated with the testing.
28	08/31/09	C Coggins	Docu-ment Defect	Closed	Unity 4.0 Discrepancy Report 10/28/08 (SysTest)  EMC Qualification Test Report ES&S Voting System,M100 060530-1050 6/29/06 (Criterion)	<p>Potentially reusable Unity 4.0 hardware test results contain no identification of the mitigation manufacturing change note.</p> <p>On pg 48 of the sub-contractor (Criterion) report mitigation occurred in the RF Immunity Test (Stewart part No. 28S0670-000 flat split type ferrite placed on ribbon cable close to J8). There is no identification of an Engineering Change corresponding to the mitigation.</p>	v.1: 9.6.2.6.e The ITA shall evaluate data resulting from examinations and tests employing the following practices: Any and all failures that occurred as a result of a deficiency shall be classified as purged, and test results shall be evaluated ...if the 1) vendor submits a design, manufacturing ... change notice...	9/8/09 -A copy of ES&S ECO 682, images of the ferrite and SysTest ECO 682 Completed Evaluation was provided by ES&S	9/8/09 Accept CEC Verified that ECO 682 documentation corresponds to the mitigation described on pg 48
29	09/01/09	S.Sivixay	Docu-ment Defect	Closed	System Limitations Unity v.3.2.1.0 3/11/09	The maximum candidates/counters allowed per election is blank on the Model 100 system limitations.	v.2: 2.3 The vendor shall provide a listing of the system's functional processing capabilities,	MDN 2009.09.25- OVR02_SystemLimitis Rev5.0 -- • Updated Section 2.2, Model 100	Accept 10/12/09 SJ: Verified System Limitations Unity v. 3.2.1.0 9/28/09

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							encompassing capabilities required by the Standards and any additional capabilities provided by the system such as candidate counters per precinct	System Limitations table to specify 21,000 as the maximum value for candidates/counters allowed per election. This is an ERM system limitation.	contains M100 maximum candidates/ counters allowed per election
30	09/01/09	M.Warner	Informational	Closed	C M100 5.4.1.0.2 Source Code Review - deleted modules not included in system changes.	C M100 5.4.1.0.2 Source Code Review - deleted modules not included in system changes.  Modules <i>crc.h</i> and <i>crc.c</i> were deleted in C M100 5.4.1.0.2 source code, but system changes listed in the Change Release Summary Changes 5.4.0.0.27 to 5.4.1.0.2 say "No Modules Deleted".  <i>In ES&amp;S Configuration Management Plan Unity v. 3.2.0.0 document, version 4.0, dated May 21, 2009, in the 1.1.1. CM Organization – Software and Firmware Development section, element "Technical Communications" says "Develops baseline system documentation based on design provided by Product Management, monitors system changes, provides quality control for technical and administrative documentation generated by other organizations, and implements documentation changes in response to system changes and audits." ES&amp;S did not follow its procedure.</i>			9/1/09 Accept MW Verified revised change notes identifying the deleted modules.
31	09/04/09	S.Sivixay	Document Defect	Closed	ES&S Model 100 System Ops Procedures FW V.5.4.0.0 HW Rev 1.3 8/11/09	256KB PC memory cards are not supported by the M100 but Ch 3 of the TDP states that the M100 does support 256KB PC memory cards.	v.2: 2.8.5.g The vendor shall provide documentation of system operating procedures that meets the following requirements: e. Define and illustrate procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved (such information shall be provided for the interaction of the system with other	DJZ - 9-18-09 - M100 SOP - Ch 3: Description of M100; pg 12. Updated the PCMCIA minimum memory on the card should be 512KB	Accept 10/5/09 CEC Verified the minimum memory in the 9/18/09 SOP

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							data processing systems or data interchange protocols as well);		
32	09/04/09	K. Wilson	Document Defect	Closed	Hardening Procedures for the Election Management System PC 3/31/09	Required Materials List states "Pentium Dual Core (or better)" This requirement contradicts the requirements stated in the "Hardware Environment and Constraints" of the Unity 3.2 documentation which only specifies an XP Platform. Hardware delivered by ES&S to date does not meet this new hardware environment.	v.1:8.3.1 The vendor shall describe the procedures and conventions used to: b. Uniquely number or otherwise identify configuration items; and...	PMZ 2009.09.25- SSS08_HardeningProcedures Rev 9.18.2009 -- • Updated Section 3.2, to specify "Pentium processor or better," rather than "...dual-core or better."	Accept 10/5/09 KGW Verified response is reflected in the 9/18/09 procedure
33	09/04/09	K. Wilson	Document Defect	Closed	Hardening Procedures for the EMS PC 3/28/09	The hardening document in Section 2.5.D refers to the "ES&S Software Installation Order" document. We cannot find this document in our TDP.	v.2:2.1.1.1 At minimum, the TDP shall contain the following documentation: ... g. User/system operations procedures	PMZ 2009.09.25- Added to the TDP as "U3210_SSS09_Software Install Order.pdf" Rev.1.0, 9.25.2009.	Accept 10/5/09 KGW Verified receipt of SW Installation Order
34	09/04/09	Sjakileti	Document Defect	Closed	System Functionality Description Model 100 Unity v.3.2.1.0 8/11/09  ES&S SW Design Spec Model 100 Unity v.3.2.1.0 8/11/09	In the M100 SW Design Spec and System Functionality Description the OS information is inconsistent  The SW Design Spec states (section3.2) " The vote tallying software runs on the Model 100 and contains a 386EX CPU with 2 Megabytes of RAM running the QNX operating system" The SFD states (section 1.1.5.2) "The ES&S Model 100 tabulator is a self-contained system running a proprietary ES&S operating system". The use of a COTS operating system is not addressed in the system functionality description for the M100 (including v.1:2.2.5.3 : COTS General Purpose Computer System Requirements)	1. v.2: 2.2.1e: e. Identification of all COTS hardware and software products and communications services used in the development and/or operation of the voting system, identifying the name, vendor and version used for each such component, including: 1) Operating systems; V.2: 2.3.a The vendor shall organize the presentation of required capabilities in a manner that corresponds to the structure and sequence of functional capabilities indicated in Volume 1 Section 2....	MDN 200909.25 - U3210_SFD00_M100 Rev.4.0 Updated Section 1.1.5.2 to identify the M100 operating system as QNX. Added verbiage to address requirements for the three required system protections referenced in the VVSG (Authentication, Audit and execution of only intended and necessary processes). This content was already present in other sections of the M100 Functional Specification but recompiled under Section 1.1.5.2 to address the referenced requirement.	Accept 10/5/09 KGW Verified response is reflected in SFD Rev.4.0
35	09/04/09	K. Wilson	Document Defect	Closed	SW Design Spec ERM Unity v. 3.2.0.0 6/23/09 [SDS]  Hardening Procedures for the EMS PC 3/28/09	The Hardening document in Ch 2 and Ch 5 discusses the multi-user capabilities of ERM and in particular references the "Cobol's file and record locking features". The SDS document does not provide sufficient information on how the ERM application implements these features in sufficient detail for iBeta to validate or	v.1:2.2.1.a Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and	GLW - 05.04.2010 - The ERM SDS, Section 3.3 has been updated to provide additional implementation detail regarding File Sharing, File locking and Record Locking employed by	Accept 5/7/10, AM ad Verified t SW Design Spec ERM 3.2.1.0 Rev 7.0, 5/4/10 addresses a) - locking is pessimistic b) - record and file

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
					Hardening]	<p>test the impact of multi-user access upon the integrity and accountability of ERM functionality. In addition to multi-user access in a functional test (which may or may not exercise race conditions associated with multi-user access to the same file or record in a database), we propose to examine the documentation and source code. Such information that is pertinent (and not found) is the:</p> <ul style="list-style-type: none"> <li>a) the nature of the COTS locking (optimistic or pessimistic),</li> <li>b) whether file, record or page level locking is implemented,</li> <li>c) overall manufacturers strategy of locking (which is usually related to optimistic or pessimistic),</li> <li>d) expected response(s) of the system when a collision occurs (i.e. recovery v.1.2.2.3.a) and</li> <li>e) any other business rules the designer/developer considers relevant. In regards to e, an example would be the names of any modules, objects or methods specifically written to address the multi-user nature of the application that are shared and used throughout the ERM application.</li> </ul> <p><b>Rejected KGW 2/22/10:</b> Reviewed SDS v.4.0 1/8/10, Hardening v.2.2 2/18/10 and source code review:  a, b, c, d ) Changes do not explicitly address the detail identified above and how the programmer is to implement multi-user data integrity</p> <p><b>Rejected AM 4/6/10:</b> Reviewed supporting documentation in "U3210_FileSpecs_DISC35_20100309": These documents comprise text search results of source code showing where files are opened with or without lock or busy, and a spreadsheet listing affected modules. Location of locking is not sufficient. In order to test file locking iBeta needs to understand the operating system or other implementation details of</p>	<p>accountability</p> <p>v.2.2.5.8 The vendor shall identify and provide a diagram and narrative description of the system's databases, and any external files used for data input or output. The information provided shall include for each database or external file: ...e. Details of ... their specifications, including: ... 7) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply;</p> <p>v.1:7.7.a To meet documentation requirements, vendors shall provide complete product documentation with each voting systems or components, as described Volume II, Section 2 for the TDP. This documentation shall:</p> <p>a. Be sufficient to serve the needs of the ITA ...</p>	<p>the ERM application software as provided by the COTS RM/Cobol language and Runtime provider, Liant, now owned by Micro-Focus, Inc. The overall solution is a combination of capabilities of the Runtime, the file sharing features provided by this Cobol language and the manner in which these capabilities are implemented within the application (ERM). This additional information specifically addresses items a, b, c, and d below:</p> <ul style="list-style-type: none"> <li>a) the nature of the COTS locking (optimistic or pessimistic)</li> <li>b) whether file, record or pg level locking is implemented</li> <li>c) overall manufactures strategy of locking</li> <li>d) expected response(s) of the system when a collision occurs</li> </ul> <p><b>MDN - 03092010 -</b>  Supporting documentation provided on 03.09.2010 under the folder titled "U3210_FileSpecs_DISC35_20100309"</p> <p><b>MDN - 1.18.2009 -</b>  Updated document delivered with TDP Rev7 1.12.2010. See revision description below.</p>	<p>locking are implemented via region (page) locking based on COTS vendor algorithm</p> <p>c) - default strategy in a shared environment is automatic single record locking; one program (UPDELC) in the source code specifically invokes automatic multiple-record locks</p> <p>d) - response to a collision is to return a status 99. This is consistent with the source code</p> <p><b>2/22/10 KW e) Accept</b>  - SDS v.4.0 1/8/10 verified mixed into code using CHECKERR</p> <p><b>Reject AM 4/6/10</b></p> <p><b>Reject KGW 2/22/10</b></p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p><i>the locking mechanism. This low level detail has not been providing for the items identified above (a, b, c, d).</i></p>		<p><i>GLW 10.28.2009 -- Updated the ERM SDS, Section 3.3 Operational Considerations, to include a detailed description of the RM/Cobol language and runtime facilities provided that enable applications to be developed that allow multi-user access to the application. This section contains information on the appropriate use of file and record locking within the application software to ensure system integrity when multiple users are concurrently accessing data within the system. Under separate cover, information will be provided to iBeta that documents the Cobol modules that perform file and/or record locking, and perform the required routines when files and/or records are accessed and cannot be read due to another user having the file and/or record locked.</i></p>	
36	09/08/09	J. Garcia	Informational	Closed	Hardening Procedures for the EMS PC 3/8/09	<p><i>The documentation does not provide an option to upgrade from SP2 to SP3</i></p> <p><i>In Ch 2 it states that the PC must be wiped and to install SP3. In this case a jurisdiction currently running SP2 cannot just run the updates for SP3 as permitted in the Unity 3.2.0.0 hardening procedure.</i></p>		<p><i>PMZ 2009.09.25- For Unity 3.2.1.0, ES&amp;S is requiring Service Pack 3 as a baseline system requirement (see the system overview and SSS). Wiping the PC prior to installing the OS is a recommended security procedure that is not dependent on the OS.</i></p>	<p><b>10/5/09 Accept: CEC</b> <i>Informational disclosure, option remains available in the Unity 3.2.0 configuration</i></p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
37	09/14/09	J. Garcia	Document Defect	Closed	Hardening Procedures for the EMS PC 3/8/09	On pg 4 and 12 of the Hardening Procedures it mentions a document called "ES&S Software Installation Order" that has not been delivered to iBeta.	v.1:9.2 The vendor shall submit to the ITA documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the ITA for system qualification testing.	PMZ 2009.09.25- Added to the TDP as "U3210_SSS09_Software Install Order.pdf" Rev.1.0, 9.25.2009.	10/5/09 Accept: CEC duplicate of #33
38	09/14/09	J. Garcia	Document Defect	Closed	Hardening Procedures for the EMS PC 3/8/09	The Hardening Procedures and AIMS Election Guide are inconsistent.  On pg 4 of the Hardening Procedures it does not state that Microsoft Visual Studio .NET 2003 is required however, the AIMS Election Officials Guide AQS-13-5001-208 section 3.1.2 Software states: AIMS requires the following external software applications: • Microsoft Excel version 5.0 or greater • Microsoft Visual Studio .NET 2003 • SanDisk Drivers for writing to Compact Flash Cards	v.2: 2.6.4 The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure software (including firmware) installation to meet the specific requirements of Volume I, Section 6.4 of the Standards. This information shall address software installation for all system components.	MDN 2009.09.25- This information was added in error to the AIMS Election Officials Guide. The VAT Preview portion of AIMS requires Microsoft .NET Framework v. 1.1, not Visual Studio 2003 .NET. .NET Framework v. 1.1 is automatically installed with AIMS. The Election Officials Guide had been updated to correct this information.	Accept 10/13/09 SJ: Verified the corrected AIMS software requirements are in the AIMS Election Official's Guide Rev.17
39	09/14/09	J. Garcia	Document Defect	Closed	Hardening Procedures for the EMS PC 3/8/09	On pg 76 of the Hardening Procedures it mentions ElectionWare and DSIM. Neither product is supported in Unity 3.2.1.0. ElectionWare is mentioned on pg 4, 12 and 22.  <b>10/26/09 Reject C Coggins</b> - These products are not in the ES&S application for Unity 3.2.1.0. Assessment of materials submitted for testing are limited to the products identified on this application unless an exception is granted and provided by the EAC. The EAC has not provided an exception for these products.  <b>1/29/10 Reject K Austin</b> - a word search found that there is still a reference to Electionware on pg 51.	v.1:9.2 The vendor shall submit to the ITA documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the ITA for system qualification testing.	DWH - 2.16.2010 - See the latest submission of the Hardening document. The word search may not have been done on the latest document.  MDN - 2.11.2010 - Final ElectionWare reference removed. See U3210_SSS08_Hardening Procedures Rev.2.1 submitted with TDP Rev7a2 2.8.2010  MDN - 1.18.2009 - References to non-supported products removed. Revised system hardening procedures provided with TDP Rev7a1 1.18.2010.	Accept 02/16/10 SLE: Verified in the Hardening Procedures EMS PC Unity 3.2.1.0 v.2.1 02/08/10 documents that ElectionWare and DSIM was no longer present.  Reject 1/29/10 KA  Reject 10/26/09 CEC

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								pmz20091013 - The document also indicates that only those products licensed and included for the user/version are to be used. There is no requirement that the document not mention MORE than the client needs.	
40	09/16/09	J. Garcia	Docu- ment Defect	Closed	Hardening Procedures for the EMS PC 3/8/09	On pg 11 number 5.c of the Hardening Procedures it mentions an application call "ES&S Application Audit Logs". This product has not been delivered nor is it identified in the EAC Application for Unity 3.2.1.0  <b>10/26/09 Reject C Coggins</b> - No documentation was found identifying the versions that include and exclude the "ES&S Application Audit Logs"	v.1:9.2 The vendor shall submit to the ITA documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the ITA for system qualification testing.	<b>MDN - 1.18.2009</b> - Reference to "Application Audit Logs" removed. Revised system hardening procedures provided with TDP Rev7a1 1.18.2010. <b>MDN 2009.09.25</b> - This section refers to the application audit logs configured with Unity Event Log Service a Windows service included in some versions of the Unity voting system. This service is not included with the Unity 3.2.1.0 system configuration. The requirement for installing application audit logs is followed by the phrase, "..., if they are part of your version ..."	<b>Accept 01/29/10 KA</b> Verified in the Hardening Procedures for EMS PC 1/18/10 that reference to "Application Audit Log" has been removed.  <b>Reject 10/26/09 CEC</b>
41	09/18/09	J. Garcia	Docu- ment Defect	Closed	Hardening Procedures for the EMS PC 3/8/09	On pg 11 in ch2 of the Hardening Procedures it mentions a document called "System Validation document" that has not been delivered to iBeta.  <b>10/13/09 Rejected SJ</b> : This document U3200_SSS05_Unity workstation validation guide is not delivered in 3.2.0.0 or 3.2.1.0 TDP	v.1:9.2 The vendor shall submit to the ITA documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the ITA for system qualification testing.	<b>MDN - 1.18.2009</b> - Reference to system validation documentation removed. Revised system hardening procedures provided with TDP Rev7a1 1.18.2010. <b>MDN 2009.10.30</b> - The referenced system validation	<b>Accept 01/29/10 KA</b> Verified in the Hardening Procedures for EMS PC 1/18/10 that reference to the system validation document has been removed.  <b>Reject 10/13/09 SJ</b>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								documentation for Unity 3200 was provided to the EAC on 07.08.2009. ES&S will provide copies for the U3210 system. <b>MDN 2009.09.25-</b> System validation documentation refers to "U3200_SSS05_Unity Workstation Validation Guide" delivered for the Unity 3200 system.	
42	09/18/09	M.Warner	Document Defect	Closed	Hardening Procedures for the Election Management System PC 9/8/09	In Ch 8 in the hardening document, the first paragraph refers to three versions of Windows hardening settings, one for Windows XP stand-alone, one for the networked Windows XP EMS PCs (peer to peer), and one for Windows 2003 Server, but only two listings are described. One for the Windows XP Stand-alone Script, and one for the Windows 2003 Server Network. There is no mention of the script used for the networked Windows XP EMS PCs.	v.2.2.1.1.1 At minimum, the TDP shall contain the following documentation: ... g. User/system operations procedures	pmz20091013 - This was an error in the document format software. The omitted information has been added back in.	<b>Accept 10/22/09 JG:</b> Verified Windows XP Peer-To-Peer Network scripts have been added 10/16/09
43	09/18/09	M.Warner	Informational	Closed	Hardening Procedures for the Election Management System PC 9/8/09	In Ch 2 in the hardening document, in the Harden the Windows XP Operating System section, in step 5.C, in the steps described for granting rights to registry keys, step 1 says to "Select Start - Run and enter reged32." There is no reged32 in Windows XP, but there is regedt32.		pmz20091013 - The typographical error has been corrected.	<b>Accept 10/22/09 JG:</b> Verified 5.c step 1 typo reged32 has been changed to regedt32 in the 10/16/09 version
44	09/18/09	M.Warner	Document Defect	Closed	Hardening Procedures for the Election Management System PC 9/8/09	In Ch 1 in the hardening document, a list of "ES&S Installation documents" mentions a document named "ES&S Unity Event Logging Service System Operations Procedures" that has not been delivered to iBeta.	v.1:9.2 The vendor shall submit to the ITA documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the ITA for system qualification testing.	<b>MDN20091019 - Unity Event Log Service is not included with the Unity 3210 system configuration. The list of required documents is preceded by the statement, "ES&amp;S Installation Documents, depending on your configuration" in Hardening Procedures for the EMS PC 10/16/09</b>	<b>Accept 10/23/09 SLE:</b> Verified the statement "ES&S Installation documents, depending on your configuration" in Hardening Procedures for the EMS PC 10/16/09
45	09/18/09	M.Warner	Document Defect	Closed	Hardening Procedures for the Election Management System PC 9/8/09	In Ch 12, Locking Down Directories, step n. says that for the ERM executable, deny the execution rights of the ElectDefine group by disabling it's access to C:\apps\less\urs\laero.cob, but then	v.1:9.2 The vendor shall submit to the ITA documentation necessary for the identification of the full system configuration	pmz20091013 - Although a trained system administrator should not need more, a description of how to do	<b>Accept 10/23/09 SJ:</b> Verified detail for setting up access rights is provided in Hardening Proc

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						does not provide instructions for "disabling access"	submitted for evaluation and for the development of an appropriate test plan by the ITA for system qualification testing.	this has been added to this chapter.	10/16/09
46	09/18/09	J. Garcia	Document Defect	Closed	EDM System Ops Procedures Version 7.8.1.0 May 26, 2009	<p>The EDM System Operations document does not provide any information on a networked system.</p> <p>On pg 44 in Ch 5 (installation) under Security Protocols states "Install EDM on a stand-alone (non-networked) PC". The documentation has not been updated to reflect the Peer to Peer or Server network setup.</p>	v.2.2.8.5.a Operating Procedures  The vendor shall provide documentation of system operating procedures that meets the following requirements: a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation.	DJZ - 10-20-09 - EDM SOP v. 7.8.1.0 - In Ch 5: Installation - pg 44 added EDM can be installed on a stand-alone PC or Peer-To-Peer Network. Also added NOTE: Refer to the Hardening Procedures for the Election Management System PC document for further information	Accept 10/22/09 JG: Verified pg 44 in Ch 5 now states "Install EDM on a stand-alone (non-networked) PC or as part of a Peer-To-Peer Network." in Hardening Proc 10/16/09
47	09/18/09	J. Garcia	Document Defect	Closed	HPM System Ops Procedures Ver. Rel. 5.7.1.0 May 11, 2009	<p>Part 2 section Install RM/Cobol 11.01 for 32-bit Windows states to:</p> <p>1. Insert the installation CD into the CD-ROM drive.</p> <p>2. Click Start on the Windows taskbar and select Run to open the Run window.</p> <p>3. Select Browse to locate the CD Rom Drive on your PC. Find the RMCOBOL11RP folder and double-click to open the folder. Double-click SETUP.EXE in the RMCOBOL folder to place it on the open path:</p> <p>The install would not process when following these steps. RMCOBOL would install when the RMCOBOL11RP folder was copied from the CD to the C drive and the Setup.exe was run.</p> <p><b>Rejected 10/23/09 SJ:</b> RMCOBOL 11.01 runtime system (setup.exe) is a download from Micro Focus. The hash of the setup.exe is "983b8a0a6f2441346400cbe6af6f63e57a580cb2" which matches the file on the CD. When we try to run the setup.exe from the CD, it tries to write or create a folder on the CD. The setup.exe runs from the CD, however it fails when it tries to write temporary files to the CD drive.</p> <p><b>Rejected 11/11/09 SJ :</b> iBeta received</p>	v.2.2.8.5.a Operating Procedures  The vendor shall provide documentation of system operating procedures that meets the following requirements: a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation.	<p>DWH - 01/28/10 - Our RMCOBOL customer install procedures reference a setup.exe which is one of the files extracted from the self-extracting setup.exe you downloaded from Micro Focus. It is unfortunate both files have the same name. The size for the customer setup.exe should be approximately 59,904 bytes and not 8,095,622 bytes. Our customer installation CD does not contain the self-extracting setup.exe.</p> <p><b>DJZ - 10/16/09 -</b> The instructions for the installation of RM Cobol are correct for the CDs that the user would receive. The files on the CD may have been copied incorrectly, which could cause the issue with not being able to</p>	<p>Accept 03/04/10 JG &amp; SJ</p> <p>The ES&amp;S customer installation CD &amp; the Downloaded RMCOBOL hashed and the hashes matched. ES&amp;S customers are provided with the RMCOBOL CD with the purchase of Unity 3.2.1.0. ES&amp;S customers would not need to download the SETUP.EXE from Micro Focus. Customers can validate its COTS with a hash check.</p> <p><b>Reject 02/24/10 SJ &amp; JG</b></p> <p><b>Reject 11/11/09 SJ</b></p> <p><b>Reject 10/23/09 SJ</b></p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>the RM/Cobol runtime system installation CD from ES&amp;S, the content of this CD is extracted from setup.exe(which iBeta downloaded from Micro Focus, size of this setup.exe is 8,095,622 bytes, right now iBeta is running this setup.exe from the CD). There is no instruction for extracting this setup.exe and burn the extracted folder "RMCOBOL11RP" to CD.</p> <p><b>Rejected 02/24/10 SJ &amp; JG:</b> The HPM SOP (Ver. Rel. 5.7.2.0 2/12/10) and ERM SOP (Ver. Release 7.5.6.0 2/12/10) does not reflect the procedure to download from Micro Focus the SETUP.EXE with 59.904 bytes.</p>		<p>open it from the CD. The CD was tested here as it is sent to the customer and it worked correctly.</p> <p><b>SLM 10.29.09 -</b> It is not an acceptable practice for a customer to download RM/Cobol 11.01 from Micro Focus. ES&amp;S will provide iBeta an installation CD. This is the same installation CD and process that a customer would follow.</p>	
48	09/18/09	J. Garcia	Document Defect	Closed	AutoMARK Information Management System Election Official's Guide Rev 16	<p>On pg 18 of the AIMS Election Officials Guide AQS-13-5001-208-R documentation it states "AIMS requires the following external software applications: • Microsoft Visual Studio .NET 2003" and a note stating "Download Visual Studio .NET 2003 from <a href="http://www.microsoft.com/downloads/details.aspx?familyid=69d2219f-ce82-46a5-8aec-072bd4bb955e&amp;displaying=en">http://www.microsoft.com/downloads/details.aspx?familyid=69d2219f-ce82-46a5-8aec-072bd4bb955e&amp;displaying=en</a>" however, this download is only an update (service pack1) and not Visual Studio .NET 2003.</p>	<p>v.2.2.8.5.a Operating Procedures</p> <p>The vendor shall provide documentation of system operating procedures that meets the following requirements:</p> <p>a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation.</p>	<p><b>MDN 2009.09.25-</b> This information was added in error to the AIMS Election Officials Guide. The VAT Preview portion of AIMS requires Microsoft .NET Framework v. 1.1, not Visual Studio 2003 .NET. .NET Framework v. 1.1 is automatically installed with AIMS. The Election Officials Guide had been updated to correct this information.</p>	<p><b>Accept 10/13/09 SJ:</b> Verified addition of Visual Studio .net 2003 in AIMS software requirements.</p>
49	09/18/09	J. Garcia	Document Defect	Closed	AutoMARK Information Management System Election Official's Guide Rev 16	<p>On pg 18 of the AIMS Election Officials Guide AQS-13-5001-208-R documentation it stats "AIMS requires the following external software applications: • Microsoft Excel version 5.0 or greater" however, this is an optional external software application.</p>	<p>v.2.2.8.5.a The vendor shall provide documentation of system operating procedures that meets the following requirements: Provides a detailed description of procedures required to initiate, control, and verify proper system operation.</p>	<p><b>MDN 2009.09.25-</b> Updated verbiage to indicate that the Excel install is optional rather than required.</p>	<p><b>Accept 10/13/09 SJ:</b> Verified there is documentation stating that Excel is optional in AIMS Election Official's Guide Rev.17</p>
50	09/25/09	K. Wilson	Document Defect	Closed	Model 100 Validation Guide 9/22/09	<p>Evidence that the boot-block source code is COTS has not been provided.</p> <p>The boot-block.hex file obtained during</p>	<p>v.1: 9.5.1 All products custom designed for election use shall be tested in accordance with</p>	<p>ERW 10-4-2009 The boot block.hex file was developed by the original</p>	<p><b>Accept 12/11/09 CEC &amp; KW</b> Verified a letter from Pivot stating the boot-</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>the validation procedure validates against the boot-block.hex file delivered by Pivot on 9/22/09. The trusted build of M100 v.5.4.1.0 does not contain the binary image for the boot-block in either the PBC5410.hex or PBC5410.PCM files. We therefore conclude that we do not have the source code for the boot-block. In regards to the boot-block source code, we must have either a) a statement from Pivot that the boot-block delivered on 9/22/09 is COTS and used in commercial applications other than elections or b) the source code for the boot-block. If the boot-block is not COTS then it must be created into a firmware image using a Trusted Build and then compared to the image currently loaded and validated in the M100.</p> <p><b>Rejected KGW 11/3/09 -- An affidavit from ES&amp;S is not sufficient. Documentation must be from the boot-block.hex manufacturer</b></p>	<p>the applicable procedures contained in this section. COTS hardware, system software and communications components with proven performance in commercial applications other than elections, however, are exempted from certain portions of the test as long as such products are not modified for use in a voting system.</p> <p>v.2:5.2 ... Unmodified, general purpose COTS non-voting software (e.g., operating systems, programming language compilers, data base management systems, and Web browsers) is not subject to the detailed examinations specified in this section. However, the ITA shall examine such software to confirm the specific version of software being used against the design specification to confirm that the software has not been modified. Portions of COTS software that have been modified by the vendor in any manner are subject to review.</p> <p>Unmodified COTS software is not subject to code examination.</p>	<p>designer/manufacturer for a board using common COTS parts and Operating System as was typical of the times. Any person or business working with the same parts and OS in the same way is free to use the boot block contents as posted on the manufacturer's web site.</p> <p>The designer/manufacturer do not have the original source code used to build the boot block and the common parts used on the main board are no longer available.</p> <p>As states in v.2:5.2... portions of COTS software that have been modified by the vendor are subject to review.</p> <p>The vendor (ES&amp;S) has never modified the work from the original designer/manufacturer. ES&amp;S is willing to sign an affidavit to this effect.</p>	<p>block.hex file is COTS and "was written to work with any application of this memory device and not solely dedicated for the ES&amp;S M100"</p> <p><b>Reject 11/3/09 KGW -</b></p>
51	09/25/09	K. Wilson	Document Defect	Closed	Model 100 Validation Guide 9/22/09	<p>We are missing the COTS documentation supporting the TDP statements that the boot-block portion of the M100 firmware is non-writable after manufacturing is complete.</p> <p><b>Rejected 11/5/09 KGW -- a) Response to #50 is N/A to this discrepancy. The</b></p>	<p>v.2:2.9.1 The vendor shall describe the structure and function of the equipment (and related software) for election preparation, programming, vote recording, tabulation, and reporting in sufficient detail</p>	<p><b>SLM 1.28.2010 - Please see submitted Intel Boot Block Flash Memory Data Sheet data July 1997,</b></p> <p><b>ERW 11.20.2009 - Please reference M100</b></p>	<p><b>Accept 02/17/10 JG KA</b></p> <p>Verified COTs document "M100MemoryDatasheet" was delivered and verifies the statement of the over-write</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>"Model 100 Validation Guide 10/30/09" now contains the statement . "This section [of flash memory] is Electrically Protected and cannot be over-written by software". This statement alone cannot be accepted without backed up of COTS documentation for the Intel flash memory chip (i.e. the datasheet).</p> <p><b>Rejected 11/29/09 kgw</b> -- did not find data sheet in TDP submitted with the response</p>	<p>to provide an overview of the system for maintenance, and for identification of faulty hardware or software.</p>	<p>Memory Data Sheet - Intel Boot Block Flash Memory Family - Section 2.1.1 Pg 13. This data sheet will be submitted as supporting documentation.</p> <p><b>SLM 10.29.09</b> - See ERW 10-4-09 response to #50 above. Please review ES&amp;S Affidavit dated 10/29/09.</p>	<p>protection.</p> <p>[Reject 11/5/09 KGW] [Reject 11/30/09 KGW]</p>
52	09/25/09	K. Wilson	Functional Defect	Closed	M100 Security - Serial Port connecting an external modem v.5.4.1.0	<p>The M100 serial port is open when connected to an external modem.</p> <p>In the M100 - Serial port test we attached an external modem. The M100 answered the modem ring and carrier (CD) was established. The test was executed with a US Robotics 5686 serial modem. A report of DTR High verifies the M100 is instructing the modem to answer the call. When connected to a PC, the USRobotics does not report DTR high. When connected to the M100 the USRobotics reports DTR high.</p> <p>Note: This test was performed after the polls were closed with the M100 on the "Polls Closed" Menu that included "Send Results." Calling was from a laptop through a PBX Teltone TLS 5. (Normally the modem test case continues with a serial port test over the telecommunications line, but because Unity 3.2.1.0 does not include any telecommunications the test was halted at the point that the CD occurred. In order to validate our test method, we verified that a PC (with a USB-Serial port converter) does not answer the modem as configured.</p> <p><b>Rejected 10/5/09 KGW</b> -- This response doesn't address contradictions between the document Disclaimer, which identifies the exclusion of "remote</p>	<p>v. 1:2.2.1.b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.</p> <p>v. 1:Section 5 Telecommunications</p> <p>v. 1:6.5 Telecommunications and Data Transmission.</p>	<p><b>GLW 01.13.2010:</b> The M100 firmware has been changed to not load the serial port driver at the time the M100 is powered up. This results in the serial port effectively not being part of the M100 configured system. (ENH17329) This is implemented in firmware version 5.4.2.0.</p> <p><b>ERW 11.20.2009</b> -- Please reference supporting document titled M100 Serial Port Connection in conjunction with the below information. Although the signals on the interface may show DTR active and carrier may be present when connected, the M100 will NEVER answer an incoming call as there is no resident software that enables this ability. The only software routine that controls the modem is "comms.c". No existing firmware</p>	<p>Accept 02/09/10 JG KW</p> <p>Verified that the M100 did not answer the ring. In v.5.4.2.0</p> <p>[Reject 11/5/09 KGW] [Reject 11/30/09 KGW]</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>transmission of data", and this accessible public telecommunications connection. "We have shown that the system can be connected to a public telecommunications system and carrier signal (CD) obtained. Therefore the functionality contradicts v.1:2.2.1.b. In discrepancy #53 we observed that DTR is high from the time the M100 boots. Therefore the capability of the system to create and maintain an active connection to a public telecommunications system exists throughout the voting cycle. If this capability remains the disclaimer is invalid and the system would be subject to testing of the authentication and secure communication after active connection to a public telecommunications system as identified in v.1: 5 and 6.5.</p> <p><b>Rejected 11/30/09 KGW</b> -- CD indicates that carrier has been established, thus providing telecommunications capability to the device. The M100 functionally answered the phone. Whether it is the COTS OS or M100 reviewed code that answered is immaterial to the finding. The response states it is under vendor control to prevent this capability but doesn't address why this capability is necessary in the 3.2.1.0 certification. The "M100 Serial Port Connection" document was not provided with the response.</p>		<p><i>routines can access this modem control routine until the polls are closed. However, even when active, no call can be answered. Once polls are closed and after a results tape has been printed, this routine is accessed if the election definition has been set up to transfer results and data transfer can be initiated. Due to the "hard wired" protocol contained in the firmware, connection can only be established with a remote system whose communication protocol matches the proprietary "hard wired" protocol. Once connected, the ONLY data that can be transmitted is the binary results data block, known as the SPP record, which contains a list of binary counts without any content identifying what the counts are associated with. Once this 2165 byte record is transmitted, the connection is broken. There is no capability in the modem firmware routines that allows data to be received other than the handshaking that is part of the transmission protocol. The description following contains further details showing how this is</i></p>	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							<p>implemented.</p> <p>The M100 powers up the serial ports during the initial boot. When the QNX operating system starts it configures itself. QNX contains a series of function calls (an API) that applications running on the OS can use to access and use devices. In this case, the API calls are used to access the QNX serial driver, Dev.ser. This driver is started from the initialization file etc/config/sysinit with the following options:</p> <p>/bin/Dev.ser -F 3F8,4 2F8,3 2E8,5 &amp;</p> <p>In the "arguments" passed to the driver on the line, the numbers identify which serial ports to control. The 3F8 is the external serial port. The VSTL has a copy of the sysinit file as part of the code submission package. It is located in the pbc-version-cots.tar.gz bundle and the vendor has included a copy with this response.</p> <p>The serial driver creates devices in the /dev/ directory under root like: /dev/ser1, /dev/ser2, etc.</p> <p>Similar to Linux, the API allows application programs to open, read, write, and close the port like a file.</p>		

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							<p><i>It is important to note that there are *no* terminal programs started on the serial port such as telnet, login, ssh, etc. and that the initialization file controls what is allowed to run on a given port.</i></p> <p><i>Examination of the source code, in particular the attached file named comms.c shows that the application is the only program using the external serial port and only uses it for data transfer of information FROM the M100 to a host system. It does not accept information or commands. It is the vendor's opinion that the send_results_to_spr() on line 5102 of this file is a good place to start. This function shows that the code does not check or care about the serial port until it needs to initialize it, check it and send data across a modem attached to it.</i></p> <p><i>The application only opens up the modem connection from its side, otherwise, the port remains "unconnected" to the application side therefore protecting the M100 from unauthorized or unintended access attempts.</i></p>		

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							<p><i>ES&amp;S feels that understanding the workings of the OS and reading and understanding the source code should allow reviews to establish the assurance necessary to confirm the serial port will not allow any unauthorized or unintended activity and that the system works in the intended manner. The fact that a person can detect a pin or signal from the serial port output does not automatically mean that a problem exists.</i></p> <p><i>It is also important to note that the serial port on an M100 is a physically secured port. Attaching an external modem or a cable to some other device would require either an obvious physical breach of the M100. This would require unlocking the ballot box to gain access to the door securing the serial port and breaking a security seal.</i></p> <p><b>ERW 10-4-2009</b> <i>The M100 uses proprietary communications protocols and does not use standard terminal commands. While it is possible to send signals to the serial port hardware it is not possible to pass commands or actual</i></p>		

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								election data back and forth between an externally connected modem and the voting device. The M100 does function only in the intended manner. Please see additional detailed explanations of the serial communication system on the M100 in the supplied document.	
53	09/25/09	K. Wilson	Functional Defect	Closed	M100 Security - Serial Port connecting an external modem v.5.4.1.0	<p>It is possible for an "iVotronic impersonator" to send commands to the M100 as currently configured.</p> <p>M100 - Serial port test with modem. When connected to a PC, the USRobotics does not report DTR high. When connected to the M100 the USRobotics reports DTR high. This is evidence that the M100 is actively listening to the serial port. DTR is raised high when the LCD flashes "Starting Serial Driver" at power on. Examination of the M100 Software Spec indicates that this serial port is prepared to accept commands from a "supervisory" iVotronic. Evidence of such was also found in the M100 source code. Details of any authentication between the "supervisory iVotronic" and the M100 were not found. Thus this rudimentary analysis suggests that the M100 could accept commands from an "iVotronic impersonator" over the serial port.</p> <p><b>Rejected 11/5/09 KGW</b> - Cannot find documentation to support the statement "ES&amp;S has provided detailed description" please provide specific locations of the PEB-M100 authentication protocol. Based on a quick analysis of the code v.1:2.2.1.b would be an applicable requirement because of the presence of active listening to the serial port. If ES&amp;S chooses to permit active listening then</p>	<p>v.1:2.2.1.c. Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met.</p> <p>v.1:2.2.1.e Provide security provisions that are compatible with the procedure and administrative tasks involved in equipment preparation, testing, and operation.</p> <p>v.1:2.2.4.1.f Protect against any attempt at improper data entry or retrieval;</p> <p>Documentation:</p> <p>v.1:6.2.2 Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access, such as: a) Use of data and user authorization ... f) Special protocols.</p> <p>v.1:2.2.1.b. Provide system functions that are executable only in the intended manner and</p>	<p><b>GLW 01.13.2010:</b> The M100 firmware has been changed to not load the serial port driver at the time the M100 is powered up. This results in the serial port effectively not being part of the M100 configured system. (ENH17329) This is implemented in firmware version 5.4.2.0.</p> <p><b>ERW 11.20.2009</b> -- In addition to the response for item 52, the vendor points out that a person could not connect an external device, such as one that could "impersonate an iVotronic", to the serial port without detection. This would require unlocking the ballot box door and breaking a seal. The ability to sense a change in output from the low level serial port hardware pins does not violate the standards as cited in this item.</p> <p><b>ERW 10-4-2009</b> It is not possible to impersonate</p>	<p><b>Accept 02/09/10 JG KGW</b></p> <p>Verified there is no report of DTR high in v. 5.4.2.0</p> <p>[Reject 11/5/09 KGW]</p> <p>[Reject 11/30/09 KGW]</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
						<p>the scope of Unity 3.2.1.0 would need to expand to include functional security testing of the authentication and validation that the active listening is not a threat. The documentation details outlined above would need to be provided.</p> <p><b>11/30/09 KGW Rejected</b> -- In the serial port protocol, the DTR high signal indicates that the port is ready to accept input. As described in discrepancy #52 ES&amp;S has the capability to prevent this vulnerability. To proceed with testing iBeta needs disclosure of the authentication protocol and TDP changes disclosing the vulnerability and detailed "mandatory administrative procedures" for the jurisdiction to mitigate a known functional security vulnerability.</p>	<p>order, and only under the intended conditions.</p>	<p>an iVotronic. Simply because the serial port responds to a few basic hardware commands does not mean that it will respond to actual data commands. The iVotronic data is stored on a proprietary PEB that uses IRDA transfer and then serial to pass commands and data back and forth. These commands are proprietary and CRC validated. ES&amp;S has provided a detailed description.</p>		
54	09/25/09	K. Wilson	Document Defect	Closed	<p>System Security Spec Ver. Rel. 3.2.1.0 3/28/09</p> <p>Software Design Spec Model 100 Unity v. 3.2.1.0 9/3/09</p> <p>Model 100 Validation Guide 9/22/09</p>	<p>The specifications and validation procedures do not address physical security for permanently installed boot block.</p> <p>The bootstrap (Sec 5.2-5.3 of Validation Guide) which starts up the QNX BIOS is reported on the LCD display as BIOS VER 2.02 8-9-2002. The bootstrap is permanently resident (c). Following validation of the firmware (which requires opening the chassis of the M100), the documentation does not address providing measures to protect against possible alteration of the validated bootstrap code. In the event that maintenance of the M100 would disturb any physical security methods the documentation would need to further address methods to reestablish the validation (a).</p>	<p>v.1:6.4.1 a. If software is resident in the system as firmware, the vendor shall require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations;</p> <p>b. To prevent alteration of executable code, no software shall be permanently installed or resident in the system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware;</p> <p>c. The system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that</p>	<p><b>MDN 10.30.2009</b> -- Added a note following Section 3.1.1 of the Model 100 Validation Guide (U3210_SSS06_M100 Validation Guide00, Rev6.0) instructing the operator to secure the Model 100 chassis with security seals and tamper evident tape after successful execution of the system validation procedure.</p>	<p><b>Accept SJ 11/3/09</b> Verified the documentation of security seals or tamper evident tape after successfully executing the system validation process in Model 100 Validation Guide 10/30/09</p>	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							<i>this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote-counting program, and its associated exception handlers;</i>		
55	09/25/09	Sjakileti	Functional Defect	Closed	M100 Security - Serial Port connecting an external modem	<p>Removing the internal modem from the M100 does not provide complete access control to prevent modem usage in Unity3.2.1.0. It is possible to connect external modem through the serial port.</p> <p>ES&amp;S excluded modeming of results from the M100 supported functionality by removing the modem. The active send results button on the M100 permits a user to access the code to modem results functions.</p> <p><b>Rejected 11/5/09 KGW</b> -- The disclaimer at the heading of most of the TDP documents states that excluded functionality "Including remote transmission of vote data." That statement implies an expected functionality. Thus v.1:2.2.1.b is violated by the ability to transmit results by setting the phone number in HPM, connecting a modem to the M100, and pressing the button to transmit in the M100. In addition, we have shown that it is possible to hack the PCMCIA cards and could therefore place a phone number into them allowing the M100 to connect to a public telecommunications system. Given a phone number and a connected modem, the M100 will dial another computer and generate a connection over a public telecommunications network. Therefore the functionality of the system violates v.1:2.2.1.b. If this capability remains the disclaimer is invalid and the system would be subject to testing of the authentication and secure communication after active</p>	<p>v.1: 6.5.1 Voting system that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software and data function.</p> <p>V.1: 2.2.1.b To ensure security, all systems shall: provide system functions that are executable only in the intended manner and order, and only under the intended conditions.</p>	<p><b>GLW 01.13.2010:</b> The M100 firmware has been changed to not load the serial port driver at the time the M100 is powered up. This results in the serial port effectively not being part of the M100 configured system. (ENH17329) This is implemented in firmware version 5.4.2.0.</p> <p><b>ERW 11.20.2009</b> -- ES&amp;S does not feel that the standards have ever or currently express the requirement that the system protect from the election administrators or their trusted staff. The standards call for establishing documented procedures which administrators can use to provide a secure system that operates in the intended manner. The door covering the PCMCIA card contains a slot for a security seal. The procedures also call for providing physical security and limiting access to the election management software machine such as the one running HPM.</p>	<p><b>Accept 02/09/10 JG KW</b></p> <p>Verified "No modem found" displayed on the M100 when attempting to modem results with an external modem on v.5.4.2.00</p> <p>[Reject 11/5/09 KGW]</p> <p>[Reject 11/30/09 KGW]</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>connection to a public telecommunications system as identified in v.1: 5 and 6.5.</p> <p>11/30/09 KGW -- Rejected. v.1:2.2.1.b "all systems shall provide system functions that are executable only in the intended manner and order and only under the intended conditions".</p> <p>Telecommunication capabilities are excluded from the 3.2.1.0 certification. Administrative privileges and "altered cards" are immaterial to the requirement. However "altered cards" are further support that the system's providing a capability outside of the boundaries of its declared certification.</p>		<p><i>Using the seal and following documented procedures prevents users from plugging an unauthorized card in the machine and proper security measures prevent access to a system to insert the phone number and trigger the send response. This does assure that the system functions in the intended manner. Making the assumption that a person could gain unauthorized access to the EMS, break seals and insert altered cards without detection is beyond the scope of the 2002 standards.</i></p> <p><b>ERW 10/4/09</b> Please see the responses to item #'s 52 and 53 above.</p>	
56	09/25/09	Sjakileti	Functional Defect	Closed	M100 Security - System Audit Log firmware installation failures v.5.4.1.0	<p>The M100 System Audit Log does not record firmware update failures.</p> <p>The M100 contains two audit logs. One is only resident on the M100 (System Audit Log) and the other (Audit Log) resides on the PCMCIA card and the M100. This issue relates to the System Audit Log. Before loading the firmware on the M100, 1. Modified 1 bit in .PCM file in 00000100 location replacing 4D with B6, inserted PCMCIA card into the M100. The M100 rejected the modified firmware displaying an error message that the flash card crc was bad. This error message was not printed on the tape and not recorded in the System Audit Log.</p> <p>2. Modified 1 bit in .pcm file in 000000B0 location replacing first 00 with 01, inserted the PCMCIA card into M100. The M100 correctly rejected the modified</p>	<p>v.1:2.2.1.a <i>Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability</i></p> <p>v.1:2.2.4.1g: g. <i>Record and report the date and time of normal and abnormal events;</i></p>	<p><b>DJZ 02.12.2010</b> M100 SOP - Added information in Ch 10: Understanding System Messages for audit log messages.</p> <p><b>SLM 02.11.2010</b> This is implemented in the new M100 firmware version 5.4.3.0.</p> <p><b>GLW 01.13.2010:</b> The M100 firmware has been changed to immediately print audit log entries that are generated when a PCMCIA election card is not inserted in the M100. (ENH17472) This is implemented in firmware version</p>	<p><b>#1 Accept 02/16/10 JG KA</b> Verified in M100 v.5.4.3.0 the error "Flash Data CRC Bad" prints on the paper tape</p> <p><b>#2 Accept 02/09/10 JG SE-</b> There is no internal audit log as the audit log is created from the PCMCIA card, which is stated in Ch 9 of the M100 SOP 1/8/10 FW v 5.4.2.0 When there is not a proper election definition loaded onto the M100 the system will print the displayed messages and errors</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
57	09/25/	Sjakileti	Func-	Closed	M100	<p>firmware both displaying the error message module on the LCD and printing it on the tape but it did not record it in System Audit Log.</p> <p><b>Rejected 11/3/09 SJ:</b> M100 reports the firmware installation failure, this failure is an event, this event is not being logged in the system audit log (on the M100 )</p> <p><b>Rejected 11/30/09 KGW</b> -- The following requirements were appended v.1:2.1. Responses that FW installation is not within the VSS scope are rejected. v.1:2.2.4.1.g is part of 2.2 "Overall System Capabilities", It is relevant. Further 2.2.4 does not say Integrity Measures are limited to vote recording and counting, it says they ensure their physical stability and function. ES&amp;S states it is possible to maliciously subvert the audit log, but this is insufficient to preclude meeting the requirement that normal (installing FW) and abnormal events (unsuccessful attempts) be recorded.</p> <p><b>Rejected 02/09/10 JG SE.</b> V.5.4.2.0 #1 The error message "flash card crc was bad" was not displayed on the paper audit log. Same test was run and after getting the error message and selecting the "OK" button a message appeared on the paper audit log "Election Load Failed" however, the message displayed did not get written to the paper audit log.</p>	v.1:2.2.1.a Provide	<p>5.4.2.0.  <b>ERW 11.20.2009</b> -- ES&amp;S does not feel that firmware installation is part of the vote recording and counting process. The standard cited is a subsection of Volume 1 - 2.2.4 that states: "Integrity measures ensure the physical stability and function of the vote recording and counting processes." Firmware installation is a technical task and not part of the vote recording and counting process. In this particular case, it appears the reviews are suggesting that the system somehow write to a storage device that is known to the system as corrupt.</p> <p>Administrators and election officials can guarantee the validity of the firmware on the machine using the documented firmware validation process.</p> <p>ES&amp;S feels this fulfills the requirement of v.1:2.2.1a.</p> <p><b>ERW - 10-4-2009</b> The M100 system audit log is kept on the PCMCIA card holding the election data. If that card is not in the device it has no way to write to it. This is in keeping with standard practice and the M100 does report the firmware installation failure.</p>	<p><i>on the tape (paper audit log).</i></p> <p><b>#1 Reject 02/09/10 JG SE</b></p> <p><b>Reject 11/3/09 SJ</b></p> <p>[<b>Reject 11/30/09 KGW</b>]</p>	<p><b>Accept 02/09/10 JG</b></p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
09			tional Defect		Security - Audit Log installation failures	<p>election definition loading failures.</p> <p>The M100 contains two audit logs. One is only resident on the M100 (System Audit Log) and the other (Audit Log) resides on the PCMCIA card and the M100. Before loading the election definition into M100, replaced 1 bit in the election definition file on PCMCIA card and inserted into M100, M100 rejected modified election definition, displaying and printing an error message PCMCIA header section failed, but this error message is not logged</p> <p><b>Rejected 11/3/09 SJ:</b> This is not only testing the physical protection, but also accidental modification on the PCMCIA card. This event is not logged in the system audit log (on the M100)</p> <p><b>Rejected 11/30/09 KGW</b> -- As stated above, there are two audit logs. Arguments against logging to the system audit log when the other audit log (on the PCMCIA card) may be corrupt are rejected. The loading of an election is a normal event and the failure to load an election is an abnormal event.</p>	<p>security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability</p> <p>v. 1.2.2.4.1g: g. Record and report the date and time of normal and abnormal events;</p>	<p>M100 firmware has been changed to immediately print audit log entries that are generated when a PCMCIA election card is not inserted in the M100. (ENH17472) This is implemented in firmware version 5.4.2.0.</p> <p><b>ERW 11.20.2009</b> -- Please see the response to item 55. The door seal over the PCMCIA card provides the security access control to fulfill the requirement. The abnormal event cited in the second citation does not occur if the proper access controls are followed. The vote recording and counting process officially starts when an election is loaded into the machine and in the case of a corrupt card that does not happen. The M100 does check the integrity of the card during every access and notifies the user of any malfunction or corruption of the device. When the storage device is corrupt or malfunctions then it is unreasonable to expect any system to write to it.</p> <p><b>ERW - 10-4-2009</b> If the M100 detects a problem with the election data card it will not write to it. The election Audit Log is kept on the election data card and a "bad"</p>	<p><b>SJ</b> Verified: when modifying 1 bit of election data on the PCMCIA card and inserting it into the M100 (FW v 5.4.2.0) that an error displays stating "PCMCIA Header Section Failed CRC...." and it is printed on the paper audit log. CH 9 of the M100 SOP 1/8/10 FW v5.4.2.0 identifies that there is no internal audit log as the audit log is created from the PCMCIA card,</p> <p><b>Rejected: 11/3/09 SJ</b> <b>Rejected 11/30/09 KGW</b></p>	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								<p>card is rejected as required. The system audit log is kept "internally" but the data is also stored on the PCMCIA card. This data is very small and uses only a very small fixed size area in internal memory such that any new value overwrites the old. It is not like a traditional log that adds entries for subsequent events and is not useful nor designed for this purpose. The vendor feels it does meet the requirement of providing access controls that limit OR detect access by providing the ability to lock and or place a seal over the PCMCIA card slot. If properly locked/sealed the item cited would not happen.</p>	
58	9/25/09	Sjakileti	Functional Defect	Closed	M100 v.5.4.1.0 Security TC	<p>Removal of the PCMCIA card is not recorded in either audit log.</p> <p>Scanned 2 ballots on the M100, while scanning a 3rd ballot the PCMCIA card was removed. The error "PCMCIA card not inserted," is printed and displayed on the LCD. The system is halted. This message is not logged. After reinserting the PCMCIA card the event is logged as election definition loaded.</p> <p><b>Rejected 11/3/09 SJ:</b> This test is not only for physical protection but it is testing failure of the PCMCIA card during the voting process. The event is not logged in the system audit log (on the M100).</p>	<p>v.1:2.2.1.a Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability</p> <p>v.1:2.2.4.1g: g. Record and report the date and time of normal and abnormal events;</p>	<p><b>ERW 11.20.2009 --</b> By using proper security techniques, the user would not have the ability to remove the card without detection because it would be covered with a door that is secured with a security seal and a lock if the user requires. If the PCMCIA card is removed during the voting process, in addition to having to break the seal a message is printed on the M100 tape. The tape printout is part of the audit record. ES&amp;S</p>	<p><b>Accept 2/1/09 KGW</b> The PCMCIA removal prints on the M100 tape in v.5.4.2.0</p> <p><b>Reject : 11/3/09 SJ</b></p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								<p>feels the M100 does exactly what the standards require a device to do in this situation.</p> <p><b>ERW 10-4-2009</b> The PCMCIA card holds the log file. (It is possible to lock it into place with both a seal and a physical lock to prevent removal) It cannot write to something that is not there but the seal and locked compartment provide adequate access controls and properly followed prevent the situation from occurring.</p>	
59	09/25/09	K. Wilson	Docu- ment Defect	Closed	Model 100 Validation Guide 9/22/09	The "Flash Chip Serial Programming Cable" referred to in the Validation Guide is not documented in terms of its wiring or connection types. Jurisdictions performing the validation procedure will need to obtain the cable. There is no specification for the cable. Nor is it clearly identified if this is provided by ES&S or COTS.	<p>v.2.2.2.1.f. The system description shall include written descriptions, drawings and diagrams that present: Interfaces among internal components, and interfaces with external systems. For components that interface with other components ...</p> <p>v.2.2.4.2 The vendor shall provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for qualification testing</p>	<p><b>nm20091016</b> - Added Section 5.8 to the Model 100 validation guide specifying requirements for the M100 serial cable.</p>	<p><b>Accept 10/23/09 SJ:</b> Verified documentation updated with the Serial Programming Cable description in U3210_SSS06_M100 Validation Guide00 10/22/09</p>
60	09/25/09	K. Wilson	Func- tional Defect	Closed	M100 v.5.4.1.0  Security TC	M100 updated with modified firmware. Trusted build PCM file was modified by 1 bit at location 0x61CFC from 0x22 to 0x23. IBeta program M100CRC was run afterward to repair the CRC (testing willful attempt to modify the firmware). The M100 was challenged with this firmware upgrade and accepted the upgrade. Files were recorded (20090924-m100-firmupgr.zip). Upgrading the	<p>v.1.2.2.4.1.f Integrity measures ensure the physical stability and function of the vote recording and counting processes To ensure system integrity, all systems shall: f. Protect against any attempt at improper data entry or</p>	<p><b>MDN 11.23.2009</b> -- Updated documentation to match the response below in the following manner: a) Updated both the Model 100 Validation Guide Section 3.1.1 with additional procedures for physically securing</p>	<p><b>11/30/09 kgw Accept</b> - M100 Validation Guide 11/23/09 &amp; M100 SFD 11/23/09 verified the additional procedures and seals address issue descriptions a through d.</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>firmware in this manner requires physical access to the key and the PCMCIA slot. The CRC is not difficult to duplicate for a trained programmer. (Detail has been provided to ES&amp;S)</p> <p><b>Rejected 11/5/09 KGW –</b></p> <p>a) Procedures in "M 100 Validation Guide 10/30/09" [Point a] The M100 chassis is sealed, but the PCMCIA slot is unsealed. "ES&amp;S System Functionality Description M100 Unity v. 3.2.1.0 10/20/09" (SFD) Sec. 1.1.1 states that "During election use, administrators must place a security seal across the access door of the memory card to prevent unauthorized access" [Point b]. It appears this statement is attempting to reference the access door after the election definition is loaded. The procedure doesn't protect the FW from malicious update between performance of [a] and [b] nor does it address procedures for a seal to be applied explicitly to the PCMCIA compartment at [a]. Procedures sufficiently detailed to mitigate this threat were not found.</p> <p>b) Pg 10 of the M100 Validation Guide &amp; pg 2 of the SFD don't define "an approved security seal" nor "tamper-evident tape". There's no chain of evidence procedure sufficient to mitigate this threat.</p> <p>c) The overall procedure doesn't address re-test of all devices prior to the start of an election. (v.1:6.4.1.a)</p> <p>d) This discrepancy and any physical security mitigation would invalidate pg 10 of the SFD, as it no longer addresses v.1:2.2.1.d. If seals must be broken under such circumstance, and this discrepancy shows the statement "M100 has no capability to write or otherwise change the program once installed" is untrue.</p>	<p>v.1:2.2.1.a a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.</p> <p>v.1:2.2.1.b "intended manner", 2.2.1.c "preconditions", 2.2.1.d "tampering during system repair", 2.2.1.g "Provide documentation of mandatory administrative procedures for effective system security."</p>	<p>the Model 100 between system validation and Election Day. b) Updated both the validation guide (Sec. 3.1.1.) and the System Functionality Description - M100 (Sec. 1.1.1.1.) with a note regarding procurement of security seals and tamper evident tape. c) The additional procedures added Sec. 3.1.1 of the Model 100 Validation Guide include a procedure for testing the election definition prior to live voting. d) Prefaced the ES&amp;S response to requirement V.1, 2.1.1.d. with the conditional statement, "With proper physical security controls established,..."</p> <p><b>ERW 10-4-2009</b> ES&amp;S does provide a process for validating the contents of the firmware both on the PCMCIA update card and on the internal flash chip. This provides complete assurance that the firmware installed is the certified version. If a jurisdiction so chooses it can make the validation mandatory. Coupled with proper security procedures ES&amp;S believes the M100 fulfills the requirements of VVSG.</p>	Rejected: 11/6/09 KW
61	09/25/09	K. Wilson	Document Defect	Closed	System Functionality Description Model 100 Unity	a) Section 1.1.1 states that a "seal can also be placed on the access door of the memory card to keep it secure" which is	v.1:2.2.1.g Provide documentation of mandatory administrative	MDN 2009.10.30 M100_SFD00- The revision described in the	Accept 11/2/09 SJ: Verified in SFD Model 100 Unity v.3.2.1.0

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
					v. 3.2.1.0 3/11/09	not a mandatory statement.	procedures for effective system security.	response below was provided with TDP Rev5, delivered 10.22.2009. Document is U3210_SFD00_M100 Rev 5.0. The response was not included on the VSTL discrepancy spreadsheet until the current submission (TDP Rev5a1). <b>MDN 2009.10.16 M100_SFD00-</b> Updated Section 1.1.1 to mandate use of a security seal during a live election.	Rev5.0 it states seals are mandatory
62	09/25/09	M. Warner	Functional Defect	Closed	Hardening Procedures for the Election Management System PC 9/8/09	Installation of AVG Internet Security 8.5 antivirus' firewall disconnects mapped network drive.  In the peer-to-peer network, installation of the AVG Internet Security 8.5 antivirus, recommended in the Hardening Procedures for the Election Management System PC, disconnects the mapping of the network drive shared on the Unity/AIMS PC (#E030). On the Unity/AIMS PC (#E030), the folder "C:\ESS" is set to be shared in Windows XP to give network access for the "Everyone" group. The ERM PC (#E077) cannot map the shared "C:\ESS" folder as a network drive while the AVG 8.5 firewall is enabled on the Unity/AIMS PC and the ERM PC. Once the AVG 8.5 firewall is disabled on the Unity/AIMS PC and the ERM PC, the ERM PC can map the shared folder (C:\ESS") on the AIMS/UNITY PC as a network drive. The	2.8.5 Operating Procedures  The vendor shall provide documentation of system operating procedures that meets the following requirements: a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation.	pmz20091030 - Please see Ch 13, "Virus Detection Software," step 3. This step instructs the user to refrain from activating the firewall because the network configuration does not require firewall protection.	Accept 11/2/09 SJ: Verified Hardening Procedures for the EMS PC, 10/30/09 contains an instruction to disable the firewall
63	09/25/09	J. Garcia	Document Defect	Closed	E Model 100 SOP FW v.5.4.0.0 HW rev. 1.3 3/28/09 (Vol2S1 TC)	The non-support of ballot-by-style early vote option on the M100 but is not documented in the SOP.  A message appeared on the M100 stating, "Error-invalid election. The early vote option does not support ballot-by-style. Please remove PCMCIA card".	2.8.5 Operating Procedures  The vendor shall provide documentation of system operating procedures that meets the following requirements: a. Provides a detailed	DJZ - 10-16-09 - M100 SOP - Updated error codes to include the "Error-invalid election. The early vote option does not support ballot-by-style. Please remove PCMCIA card" -	Accept 10/22/09 SLE Verified the error message and solution was included in the M100 SOP 10/21/09

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
						The message does not appear in the documentation.	description of procedures required to initiate, control, and verify proper system operation.	Solution" This card cannot be used for this election. Contact ES&S technical support for assistance.		
64	10/01/09	M. Warner	Informational	Closed	Hardening Procedures for the Election Management PC 9/28/09	<p>Anti-virus for Windows Server 2003 Server not specified.</p> <p>According to the AVG 8.5 Internet Security User Manual (download at <a href="http://download.avg.com/filedir/doc/AVG_Internet_Security/avg_ais_um_a_en_85_7.pdf">http://download.avg.com/filedir/doc/AVG_Internet_Security/avg_ais_um_a_en_85_7.pdf</a>), the AVG 8.5 Anti-virus software recommended by ESS is not intended to be installed on servers. There is no recommended Anti-virus software for the Windows Server 2003 Server specified in the Windows Hardening Procedures document.</p>		pmz20091013 - The instructions for the Installation and updating of the antivirus protection have been updated.	Accept 10/22/09 SLE Verified the instructions and installation procedures for a Virus Detection Software were added to Hardening Procedures for the EMS PC 10/16/09	
65	10/01/09	J. Garcia	Functional Defect	Closed	M100 FW 5.4.1.0 Printing of audit log Vol. 4 TC	<p>M100 audit log will not print once the log is full.</p> <p>The M100 audit log is stored on the PCMCIA card. When the log is full an error is given stating, "Audit Log Full" and the M100 displays a message "System Halt - Power down the key". The M100 will not allow the user to print the audit log. There is no identified capability within the voting system to view or print the audit log in this situation.</p> <p><b>11/11/09 Reject C Coggins &amp; J Garcia</b> While we acknowledge the argument that this test may not be a real world situation, it does not exempt the system from meeting the standard. The response does not identify a method by which the system could meet these requirements on either the M100 or recovery in another manner.</p>	<p>2.2.8.1.a ...generate machine-level audit reports.</p> <p>2.2.5.1 Archive record of all system activity ... in the event of criminal or civil litigation.</p> <p>2.2.5.2.1.g The system shall be capable of printing a copy of the audit record.</p>	<p><b>GLW 01.13.2010:</b> The M100 firmware has been changed to allow the M100 operator to print the entire audit log to the M100 printer before the M100 powers down. (ENH17106) This is implemented in firmware version 5.4.2.0.</p> <p><b>ERW 11.20.2009 --</b> ES&amp;S will modify the firmware for the M100 to allow printing of the log when full.</p> <p><b>ERW 10-4-2009</b> Filling the audit log is an exercise for testing and did not represent a real-world election. The space available for audit entries on the M100 audit log storage space far exceeds the needed space for our largest customer's largest elections. In real practice, no jurisdiction</p>	Accept 02/02/10 JG Verified that when the M100 Audit log is full there is an option allowing the user to print the Audit log and audit log prints correctly  Reject 11/11/09 CEC & JG	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								<p>in any circumstance has ever come even vaguely close to using all of the available space. The archive or actual file is available but the M100 won't allow the addition of additional entries if the log space is artificially filled up.</p> <p>Given that the M100 would allow printing of a full audit log the rolls of paper necessary to print the thousands upon thousands of entries is prohibitive and is not a real-world practice. The PCMCIA cards selected for certification and use with the systems were specifically specified to be able easily accommodate the largest elections.</p>	
66	10/120 9	J. Garcia	Informational	Closed	ES&S HPM System Ops Procedures V.5.7.1.0 5/11/09	<p>The documentation states to Loading Memory Device with Parameters, select the type of drive you want to use and click OK. There is no option to select a drive.</p> <p><b>1/5/10 - Clarification JG &amp; CEC</b> The Omni drive option to select is not identified in the document.</p>		<p><b>DJZ - 10/16/09</b> - Added additional information on pg 21-23, to choose Specify Drive Type - Choose either OMNI-PARALLEL Drive or OMNI-USB Drive from the drop down menu.</p>	<p><b>Accept 11/4/09 SJ:</b> Verified H PM SOP ver. rel. 5.7.1.0 10/29/09 identifies the drive type</p>
67	10/120 9	J. Garcia	Functional Defect	Closed	HPM 5.7.1.0 precincts Vol.12 TC	<p>No error message is generated when an election with 19 precincts is assigned in HPM (system limit for M100 is 18 precincts).</p> <p>An election with 19 precincts can be assigned to a single polling place in HPM without error. The HPM limitation for election day Precincts is 18 and that is all that gets burnt to the PCMCIA card. The user is not notified that the 19th precinct was not burnt to the PCMCIA card even though that precinct was assigned to that polling place. HPM does not</p>	<p>v.1: All voting systems shall meet the following requirements for error messages:</p> <p>e. the message cue for all systems shall clearly state the action to be performed in the event that operator response is required.</p>	<p><b>DJZ 02.12.2010</b> Put in Warning message in Ch 22. The user will get a warning that they will need to go back and adjust their precincts in the polling place. Updated warning message tables in Ch 36.</p> <p><b>EBD 02.12.2010 HPM SFD</b> - Updated warning messages under section 1.1.5.1.b</p>	<p><b>Accept 02/17/10 JG</b> Verified HPM 5.7.2.0 provides the user a warning message when exceeding 18 precincts.</p> <p><b>Reject 02/02/10 JG</b></p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>generate either a warning or error message.</p> <p><b>02/02/10 Rejected J Garcia:</b> This election was configured in EDM with 19 precincts assigned to a polling place and then pulled into HPM. The user will only get the warning message if 19 precincts are assigned to a polling place in HPM or if the user makes a change to the polling places/precincts in HPM. No warning message was generated in HPM when the election was pulled from EDM and the user was able to create the PCMCIA card. The PCMCIA card was placed into the M100 and the Initial State Report printed. The report indicated that only 18 precincts were on the PCMCIA card.</p>		<p><b>SLM 01.27.2010 - If the HPM user attempts to put more than 18 precincts into a single Polling Place a warning message is displayed back to the screen. After pressing OK, only the first 18 precincts are updated into the Polling Place record. This warning message is not written to the HPM System Log, but a Polling Place Listing can be printed to audit the precincts place into each Poll. In this case, only the first 18 precincts will be listed. And, the screen only reflects the first 18 precincts as well.</b></p>	
68	10/06/09	K. Wilson	Docu-ment Defect	Closed	Hardening Procedures for the EMS PC 9/28/09	<p>Under Ch 2 "Harden the BIOS" a note appears indicating that the BIOS boot order would be modified at the end of Ch 2. However no such statement appears at the end of Ch 2 or anywhere else in the chapter.</p>	<p>v.1:2.2.1.b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.</p>	<p><b>pmz20091013 - Pg 14</b> of our version has bullet 9 which does state that the boot order should be modified.</p>	<p><b>Accept 10/22/09 JG:</b> In Ch 2 pg 14 step 9 it states, "Restart the computer and enter the BIOS configuration. Change the boot sequence to boot only from hard drive." in 10/16/09</p>
69	10/06/09	K. Wilson	Docu-ment Defect	Closed	Hardening Procedures for the EMS PC 9/28/09	<p>The laptop Dell Latitude E6400 test platform has wireless capability built in. There are no instructions in the hardening guide to disable wireless from the BIOS. Failure to disable is a configuration that is inconsistent with the scope of the voting system submitted for certification. A system that connects to public networks is subject to all telecommunications requirements.</p> <p><b>10/22/09 Rejected: J Garcia</b> Disable all network ports and modem hardware is stated however, the wireless capability is built into the laptop. In this instance a user can still access a wireless</p>	<p>v.1:2.2.1.b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.</p> <p>All requirements with connection to the public networks in v.1:Section 5 Telecommunications and v.1:6.5 Telecommunications and Data Transmission</p>	<p><b>DWH - 2.18.2010 - See the latest submission of the Hardening document. The latest Hardening document may not have been reviewed. Appendix C states if supported, wireless capabilities should be removed. The word "capabilities" was added for clarification. The reference to Section 8 was in error as it does not address this issue.</b></p>	<p><b>Accept 2/19/10 JG KA</b> Verified 'Hardening Procedures for the EMS PC' 2/18/10 Appendix C states to disable any wireless capabilities and landline modems.</p> <p><b>Reject 10/22/09 JG</b></p> <p><b>Reject 02/03/10 KA</b></p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>connection without a modem if the BIOS is not disabled.</p> <p><b>2/03/10 Rejected: K Austin</b> The Hardening Procedures still refers only to turning off the modems. Section 8.2.2 (&amp; 8.8.2) advise contacting the computer manufacturer for information on drivers. No instruction addresses disabling all wireless capabilities.</p>		<p>This issue is handled by the hardening scripts.</p> <p><b>MDN - 2.18.2010</b></p> <p>Updated document provided with TDP Rev8a2 02182010.</p> <p><b>MDN - 1.18.2009</b> - Issue corrected.</p> <p>Revised system hardening procedures provided with TDP Rev7a1 1.18.2010. See Sec. 8.8.2 for prohibition of wireless devices.</p> <p>See Sec. 9 - Appendix C for procedures for hardening the BIOS (setup 1.d)</p> <p><b>pmz20091013</b> - Pg 7 bullet 1C of our version does instruct the user to disable ALL modems.</p>	
70	10/07/09	K. Wilson	Functional Defect	Closed	EMS Windows Configuration Security TC	<p>A non-administrative user can gain complete access booting from a BartPE CD, by passing the Windows Event Log.</p> <p>On the Peer-to-Peer configuration, ERM laptop (E077 Dell Latitude) E6400 -- Using a non-admin BIOS login password the system booted from a BartPE CD in CD drive. The non-administrator had complete access to the entire system and by-passes the Windows Event Log.</p>	<p>v.1:2.2.1.a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.</p> <p>v.1:2.2.1.b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.</p>	<p><b>pmz20091019</b> - Proper execution of system hardening procedures prevents booting from CD.</p>	<p><b>Accept 10/26/09 KGW</b></p> <p>Verified that boot sequence is identified in the Hardening Procedure 10/16/09</p>
71	10/07/09	K. Wilson	Functional Defect	Closed	EMS Windows Configuration Security TC (step 3)	<p>The virus emulation program can be installed on the ERM laptop by a non-administrative user.</p> <p>In the peer-to-peer network configuration the Results User, a non-administrator, was able to run and install a virus emulation program from a USB drive. The program was installed on the ERM laptop (test unit E077- Dell Latitude E6400).</p>	<p>v.1:2.2.1.b &amp; c. b) Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.. c) Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met.</p>	<p><b>MDN - 1.18.2009</b> - Issue corrected.</p> <p>Revised system hardening procedures provided with TDP Rev7a1 1.18.2010. See Section 11, Appendix E, 1st paragraph for mandatory virus scanning for removable devices.</p>	<p><b>Accept 02/22/10 KA</b></p> <p>Verified that a non admin user is blocked from running the virus and receives the message "Windows cannot open this program because it has been prevented by a software restriction policy. ..."</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p><b>Rejected - 10/26/09 KGW --</b> The iBeta virus emulation program represents a program that is not "only intended and necessary"</p>	<p>v.1:2.2.4.1.f. Protect against any attempt at improper data entry or retrieval</p> <p>v.1:2.2.5.3 Third, the system shall be configured to execute only intended and necessary processes during the execution of election software.</p>	<p>pmz20091019 - Active virus detection software prevents execution of a virus Proper execution of system hardening procedures prevents a malicious user from running a virus.</p>	<p><b>Reject 10/26/09 KGW</b></p>
72	10/07/09	K. Wilson	Functional Defect	Closed	EMS Windows Configuration Security TC (step 4a)	<p>An ERM voting application file can be external modified and restored to with audit logging of the relevant events.</p> <p>In the peer-to-peer network configuration a voting application file was modified on the ERM laptop (test unit E077- Dell Latitude E6400) using Notepad. It was removed from the computer by USB, modified on another computer, had its date changed back to the original file date and replaced on the c:\elecdata folder. Modification was not prevented. The windows security event log did not contain any events associated with access to the file. (The file name is reported separately to ES&amp;S.)</p> <p><b>Rejected KGW 10/26/09 --</b> Qualified iBeta personnel were not instructed what folders to apply the "Turn Tracking On for a Folder" section of Ch 12. The statement "where you want to monitor changes" was not specific.</p>	<p>v.1:2.2.1.a a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability</p> <p>v.1:2.2.5.3 Second, operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object.</p>	<p><b>MDN - 1.18.2009 -</b> Issue corrected. Revised system hardening procedures provided with TDP Rev7a1 1.18.2010. See sec. 13.1.2 for procedure for activating auditing of the c:\elecdata folder.</p> <p><b>pmz20091019 -</b> Proper system configuration and execution of system hardening procedures will cause access to this file to be logged.</p>	<p><b>Accept 02/23/10 JG KA</b> Copied file to a USB and replaced with a modified file. Verified that access to the c:\elecdata file was detected and logged in the event log with the user and the file being accessed.</p> <p><b>Reject 10/26/09 KGW</b></p>
73	10/07/09	K. Wilson	Functional Defect	Closed	EMS Windows Configuration Security TC (step 4b)	<p>The a program can be executed on the ERM laptop by a non-administrative user without logging the event.</p> <p>In the peer-to-peer network configuration the Results User, a non-administrator, was able to run an executable program (notepad.exe) on the ERM laptop (test unit E077- Dell Latitude E6400). A non-administrative user should not be able to run this program. Running of this program was not logged in the Windows Event Log.</p>	<p>v.1:2.2.5.3 Second, operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object.</p> <p>v.1:2.2.5.3 Third, the system shall be configured to execute only intended and necessary processes</p>	<p><b>MDN - 1.18.2009 -</b> Issue corrected. Revised system hardening procedures provided with TDP Rev7a1 1.18.2010. See Sec. 15 for creating user groups. Execution of hardening script prevents non-administrators from activating non-essential programs.</p>	<p><b>Accepted 02/19/10 JG KA</b> Verified non-admin users could not open Notepad or other non essential applications (HyperTerminal and sound recorder). A warning message displayed and the attempt was logged in the event log.</p> <p><b>Reject 10/26/09 KGW</b></p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p><b>Rejected KGW 10/26/09 -- As in #72 the only folders to which security tracking are applied are the Unity\AuditManager folder (as stated in Ch 12 Item f and by inference from the diagram shown under "Turning Tracking On for a Folder" section 4: the C:\Unity folder.</b></p>	<p>during the execution of election software.</p>	<p>pmz20091019 - Proper system configuration and execution of system hardening procedures prevents a user from running Notepad.</p>	
74	10/07/09	K. Wilson	Functional Defect	Closed	EMS Windows Configuration Security TC (step 4c)	<p>Launching of ERM was not logged.</p> <p>In the peer-to-peer network configuration the Results User, a non-administrator, launched ERM (test unit E077- Dell Latitude E6400 laptop). Launch of the program was not logged in the Windows Event Log.</p>	<p>v.1:2.2.5.3 ... operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object.</p>	<p>DWH - 1.28.2010 - The PreInstallNetwork.EXE and PreInstallNoNetwork.EXE scripts set the Audit Policy to capture these events.</p>	<p>Accept 02/22/10 KA Verified a non-admin user (elect-results1) launching ERM is recorded in the event log.</p>
75	10/07/09	K. Wilson	Functional Defect	Closed	EMS - Network Ports Security TC	<p>Nessus was able to log in as a guest user on the ERM laptop.</p> <p>A laptop with Nessus (a network vulnerability scanning tool) was connected to the peer-to-peer network hub which included the Unity desktop (test unit E030) and the ERM laptop (test unity E077). Nessus initiated a series of automated scans to penetrate the two platforms. Access to the Unity desktop was not gained. Nessus succeeded in an SMB (Server Message Block) scan to log into the ERM laptop as a guest user using a random account.</p>	<p>v.1:2.2.1.a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability</p> <p>v.1:6.2.1.c Communications</p> <p>v.1:6.2.1.2 Voting system vendors shall:</p> <p>a. Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access;</p>	<p>pmz20091019 - Procedures for hardening the notepad and desktop are identical and should results in identical results for this test. Variance in behavior indicates that the two systems were not configured identically.</p>	<p>Accept 10/20/09 KW – Tester error. Examination of the hardening scripts indicated guest access is turned off. It is believed to have been turned back on when testers were working with the file sharing &amp; anti-virus configurations. After correcting the setting the vulnerability was not observed</p>
76	10/08/09	J. Garcia	Document Defect	Closed	Hardening Procedures for the EMS PC 09/18/09	<p>The Hardening procedures for setting up a shared drive to work between HPM and ERM are incomplete.</p> <p>On pg 13 it states, "Once an election has been created it can be published to the shared directory so that HPM burning and ERM can access it in multi-user mode. HPM and ERM access the election information from the shared network directory. Manual procedures should be used to ensure all HPM</p>	<p>V.2:2.8.5 Operating Procedures</p> <p>The vendor shall provide documentation of system operating procedures that meets the following requirements:</p> <p>a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation.</p>	<p>DWH - 2.18.2010 - See the latest Hardening document submission. The Hardening document contained a high level overview of the application requirements meant only to provide a general understanding. It is not the purpose of the Hardening</p>	<p>Accept 02/23/10 KA JG Hardening Procedures EMS PC Unity v.3.2.1.0 2/18/10 references the System Overview. As the Hardening Procedure does not detail HPM &amp; ERM application functionality this discrepancy is closed</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>changes are finished before allowing multiple-user access to the HPM data to perform burning." No procedures are identified. ES&amp;S staff provided information to complete the task. We configured the environments using the following process:</p> <ul style="list-style-type: none"> <li>• Peer to Peer: Copying the Elecdata files created by HPM on the Ballot Prep PC to the shared folder with the ERM user coping the same files from the shared folder back to the Elecdata folder on the ERM PC.</li> <li>• File Server: After installing all software and defining the "Z" drive the user copied an election (provided with the install of all Unity software) from the Elecdata folder to the shared folder. The user opened HPM, selected Change Control File, and set the Using Network to the shared drive. Then the user repeated the Change Control Files steps in ERM.</li> </ul> <p><b>2/03/10 K Austin Reject:</b> The Hardening procedure does not discuss how to set up a shared drive to work between HPM and ERM or reference other sources of this information.</p>		<p>document to explain detailed application requirements. Therefore all references to application requirements have been removed from the document. Appendix F of the Hardening document does reference the ES&amp;S Voting System Overview as the source of application requirements.</p> <p><b>MDN - 2.16.2010</b> -For server setup information see document provided with TDP Rev7a1 1.18.2010. See sec. 17 Appendix K.</p> <p><b>MDN - 1.18.2009</b> - Issue corrected. Revised system hardening procedures provided with TDP Rev7a1 1.18.2010. See sec. 16, Appendix J for updated procedures.</p>	<p>and #128 will be opened against the HPM &amp; ERM SOPs</p> <p><b>Reject KA 02/03/10.</b></p>
77	10/08/09	J. Garcia	Functional Defect	Closed	M650 v.2.2.2.0	<p>Created an election by precinct and the M650 displayed an incorrect error, "Precinct Id is Undefined".</p> <p>Created an Open Primary with Party Preference election and selected the ballot ID of "by Precinct". In ESSIM no headers were created (The ESSIM SOP documentation states that an election by Style is the only time Precinct Headers need to be created), continued to HPM and created M650 media. Loaded the election and attempted to start scanning ballots. A message displayed "Precinct ID is Undefined" and ballots will not scan. According to the M650 SOP manual "ERROR: Precinct ID is Undefined!"</p>	<p>V.1:2.2.5.2.2 Error Messages e. The message cue for all systems shall clearly state the action to be performed in the event that voter or operator response is required.</p> <p>V.1:2.2.1 Security b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.</p>	<p><b>BJ - 4.4.2010 -M650 SOP Rev April 7, 2010.</b> See Ch 5, "Operate the Scanner: Precinct Identification Header" (current pg 35). Added note regarding Mixed Mode in a By Precinct election.</p> <p><b>MDN - 1.18.2009</b> - Revised HPM documentation (changes described below) provided with TDP Rev6 (11.22.2009) and TDP Rev7 (1.12.2010).</p>	<p><b>Accept 04/14/10 JG KA – Verified in ES&amp;S Model 650 SOP FW v. 2.2.2.0 HW v. 1.1 and 1.2 4/7/10 states that the M650 does not support Mixed Mode in a By Precinct election type.</b></p> <p><b>Reject JG &amp; CEC 4/1/10</b></p> <p><b>Reject JG 11/11/09</b></p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>means: "The scanner operator ran a header ballot in mixed mode that the scanner does not recognize. The precinct ID is undefined." However, the error generated did not correctly identify the issue as no header was scanned.</p> <p><b>11/11/09 JG Rejected:</b> Pg 87 of the HPM SOP V 5.7.1.0 11/29/09 does state that the user needs to renumber their precincts in HPM. The document does not address displaying an incorrect error or that the election is set up "by Precinct" and the M650 is requiring the use of headers. Item #2 states "Don't run the election in Mixed Mode. Instead, sort your ballots by precinct, and use headers to run them." Our test case is to test Mixed Mode as this is an option supported by ES&amp;S and it is expected to run without headers per ES&amp;S documentation.</p> <p><b>4/1/10 JG &amp; CEC Rejected</b> Updated documentation does not address that the system does not support a System Type of "Mixed Mode" in a "By Precinct" Election Type.</p>		<p><b>DJZ &amp; JML 11.20.2009</b> - The election in question uses precinct IDs that do not begin with 1. The first precinct in this election is I'd as 1000. Paper ballot sequence numbers always start with Sequence 1. Starting with M650 firmware version 2.2.0.0 precinct ID must match Ballot sequence. Updated the HPM System Operations Procedures Manual, Ch 16 to address this issue.</p> <p>ES&amp;S suggests that following resolutions: Updated error in 650 SOP, pg 83. it now states: Precinct ID is Undefined - The scanner operator ran a ballot in mixed mode that the scanner does not recognize. The precinct ID is undefined.</p> <p>1. The user will receive this error on the 650 if the scanner does not recognize the ballot. 2. If the user does not re-number their precincts then they will have to use headers for the ballots to run correctly.</p> <p><b>JML 10.28.2009</b> - The election in question uses precinct IDs that do not begin with 1. The first precinct in this election is I'd as 1000. Paper ballot sequence numbers always start with Sequence 1. Starting with M650</p>	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								<p>firmware version 2.2.0.0 precinct ID must match Ballot sequence. Updated the HPM System Operations Procedures Manual, Ch 16 to address this issue. ES&amp;S suggests that following resolutions: 1. Renumber your precincts in HPM to use the sequential precinct IDs. As ballots are normally printed using successive sequence numbers, this will result in the sequence number of the ballot matching the Precinct ID code. This will enable the election to run without headers. 2. Don't run the election in Mixed Mode. Instead, sort your ballots by precinct, and use headers to run them.</p>	
78	10/08/09	Sjakileti	Functional Defect	Closed	CRC check loading an election on the M100 Security TC	<p>CRC can be modified on a PCMCIA card loaded into the M100</p> <p>By using PC Card Manager the tester copied the PCMCIA card to a file, modified one bit in location 00000040 (last bit in that row), and fixed the CRC using M100CRC (iBeta program to repair the CRC). The tester copied this modified file to the PCMCIA card and inserted the card into the M100. The M100 accepted the modified election definition (It should be noted that this test scenario is not assuming access by voters or poll workers. This test assumes technical skill and insider access by one or multiple perpetrators with senior programming knowledge that can engineer a program to repair the CRC through access to prior election artifacts as either an election official insider or a</p>	<p>v.1:2.2.4.1.f Integrity measures ensure the physical stability and function of the vote recording and counting processes To ensure system integrity, all systems shall:</p> <ul style="list-style-type: none"> <li>f. Protect against any attempt at improper data entry or retrieval;</li> <li>v.1:2.2.1.a a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.</li> <li>also v.1:2.2.1.b "intended</li> </ul>	<p><b>MDN - 2.17.2010</b> - Strengthened the language in the Model 100 SOP and System Security Specifications (Sections referenced below) to indicate that documented procedures for securing the Model 100 are mandatory.</p> <p><b>BB 02.12.2010 SSS</b> - Added M100 Security Seals section to the appendix (Ch 2, "Appendix - Model 100 Security Seals.")</p> <p><b>BB 02.12.2010 M100 SOP</b> - Added procedures for applying security seals to the Model 100 SOP (Ch 5,</p>	<p><b>Accept 2/17/10 JG KA</b></p> <p>Verified ES&amp;S System Security Spec Ver. Rel. 3.2.1.0 2/17/10 in Ch 2 and ES&amp;S M100 SOP FW v.5.4.3.0, HW Rev 1.3 2/12/10 (see discrepancy #124) both documents now enforce the use of tamper evident seals.</p> <p><b>Reject 2/17/10 JG KA [Reject 11/30/09 KGW]</b></p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>public resale of the M100. A perpetrator must have access to the PCMCIA as they are prepared for election. No attempt was made to manipulate the election. This test only identifies that the CRC can be intentionally modified without detection. Accidental corruption of the CRC is detected. )</p> <p><b>Rejected 11/30/09 KGW</b> - Documents reference the M100 in general statements regarding "proper use of seals" and "proper administrative practices", but no specific mandatory administrative procedures are outlined. Unity 3.2.1.0 Sys Security Spec 9/25/09 has an appendix chapter on the iVotronic but nothing for the M100. No information was found in the HPM or M100 System Ops Manuals (10/29/09). This vulnerability was found during functional testing. Broad "administrative practices" can't be used to mitigate a specific threat. The specific mitigation factors provide in the response aren't found in the TDP. Nothing addressing 2.2.1.d was found. The reviewer can't find "mandatory administrative procedures for effective system security." Appendix Ch 2 of the SSS (9/25/09) has Florida procedures but, they are only cited as mandatory in FL and don't specifically and objectively address this vulnerability.</p> <p><b>2/17/10 KA &amp; JG Reject</b> The ES&amp;S System Security Spec Ver. Rel. 3.2.1.0 dated 2/12/10 in Ch 2 and ES&amp;S M100 SOP FW V. 5.4.3.0, HW Rev 1.3 dated 2/12/10 states the user can or should use tamper evident seals however does not require the use of tamper evident seals.</p>	manner", 2.2.1.c "preconditions", 2.2.1.d "tampering during system repair", 2.2.1.g "Provide documentation of mandatory administrative procedures for effective system security."	"Model 100 Security Locks and Seals.") <b>ERW 11.20.2009</b> -- The sections of the VVSG cited above are subsections of Volume 1 Section 2.2. Section 2.2.1 starts specifically with the language; "System security is achieved through a combination of technical capabilities and sound administrative practices." The PCMCIA card is either kept in the presence of an authorized election official or held in the PCMCIA slot on the M100. The door covering the seal is locked behind a hinged panel on the ballot box and the door covering the PCMCIA card contains a slot for a security seal. The documentation detailing sound administrative practices calls for providing physical security and limiting access to the election management software machine such as the one running HPM. Using the seal and following documented procedures prevents users from plugging an unauthorized card in the machine and proper security measures prevent access to a system to insert a modified card. The procedures also provide	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								a method to sustain a "chain of custody" consistent with sound security practice. The locks, seals and documented procedures do assure that the system adheres to v.1:2.2.4.1f, v.1:2.2.1.1a, v.1:2.2.2.1b, c and g.	
79	10/08/09	Sjakileti	Functional Defect	Closed	CRC check loading M100 results in ERM Security TC	<p>CRC can be modified on a PCMCIA card with votes and loaded into ERM.</p> <p>Scanned couple of ballots on M100 closed the polls and removed the PCMCIA card. By using PC Card Manager copied PCMCIA card content to a file ,modified one bit in location 00000040(last bit in that row),and fixed the crc using M100CRC( IBeta program to repair the CRC). Copied this modified file to PCMCIA card and loaded the results into ERM. ERM loaded modified election results.</p> <p>(The test scenario conditions are the same as #78 except it contains election results. No attempt was made to manipulate the results. This test only identifies that the CRC can be intentionally modified without detection. Accidental corruption of the CRC is detected.)</p> <p><b>Rejected 11/30/09 KGW</b> -- Same as #78, additionally nothing was found in ERM Sys Ops Manual (11/20/09). No objective and mandatory administrative practices were found in the TDP. A specific objective vulnerability was found in functional testing and a specific objective mitigation must be provided. Statements such as "proper administrative practices" and "secure chain of custody" aren't specific requirements for mandatory administrative procedures.</p>	v.1:2.2.4.1.f Integrity measures ensure the physical stability and function of the vote recording and counting processes To ensure system integrity, all systems shall: f. Protect against any attempt at improper data entry or retrieval; v.1:2.2.1.a a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability. also v.1:2.2.1.b "intended manner", 2.2.1.c "preconditions", 2.2.1.d "tampering during system repair", 2.2.1.g "Provide documentation of mandatory administrative procedures for effective system security."	<b>MDN - 2.17.2010</b> - Strengthened the language in the Model 100 SOP and System Security Spec (Sections referenced below) to indicate that documented procedures for securing the Model 100 are mandatory. <b>BB 02.12.2010 SSS</b> - Added M100 Security Seals section to the appendix (Ch 2, "Appendix - Model 100 Security Seals.") <b>BB 02.12.2010 M100 SOP</b> - Added procedures for applying security seals to the Model 100 SOP (Ch 5, "Model 100 Security Locks and Seals.") <b>ERW 11.20.2009</b> -- ES&S does not feel that the standards have ever or currently express the requirement that the system protect from the election administrators or their trusted staff. The standards call for establishing documented procedures administrators can use to provide a secure system that operates in	Accept 2/17/10 JG KA Verified ES&S System Security Spec Ver. Rel. 3.2.1.0 2/17/10 in Ch 2 and ES&S M100 SOP FW v.5.4.3.0, HW Rev 1.3 2/12/10 (see discrepancy #124) both documents now enforce the use of tamper evident seals. Reject 2/17/10 JG KA [Reject 11/30/09 KGW]

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p><b>2/17/10 KA &amp; JG Reject</b></p> <p>The ES&amp;S System Security Specification Ver. Rel. 3.2.1.0 2/12/10 in Ch 2 and ES&amp;S M100 SOP FW V. 5.4.3.0, HW Rev 1.3 2/12/10 states the user can or should use tamper evident seals however does not require the use of tamper evident seals.</p>		<p>the intended manner. The door covering the PCMCIA card contains a slot for a security seal. The procedures also call for providing physical security and limiting access to the election management software machine such as the one running HPM. Using the seal and following documented procedures prevents users from plugging an unauthorized card in the machine and proper security measures prevent access to a system to insert a modified card. The procedures provide a method to sustain a "chain of custody" consistent with sound security practice. The procedures do assure that the system functions in the intended manner. Making the assumption that a person could gain unauthorized access to election equipment, break seals and insert altered cards without detection is beyond the scope of the 2002 standards.</p>	
80	10/12/09	J. Garcia	Functional Defect	Closed	AIMS v.1.3.157	<p>An ActiveX error displays in AIMS when logged in as "Defineuser" or "Adminuser".</p> <p>Log into Windows as either Defineuser or Adminuser. Open and log into AIMS. From the wizard menu select #4" Import vendor election data". At this point an error is given "Error! ActiveX component</p>	<p>V.1:2.2.1 Security b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.</p> <p>v.1:6.2.1.2 Voting system vendors shall:</p>	<p><b>JML 10.28.2009:</b> This issue is resolved with AIMS v 1.3.257</p>	<p><b>Accept 3/19/10 JG</b> Verified in AIMS 1.3.257 the ActiveX error did not displays in AIMS when logged in as a Define user or Adminuser</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						can't create object".	a. Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access;		
81	10/12/09	Sjakileti & J. Garcia	Functional Defect	Closed	System Admin role-Hardening Procedures for the EMS PC 9/18/09 Ch 2 section 3A	A System Administrator can access and execute all ES&S applications.  In Ch 2 section 3A (hardening procedures) it states "The System Administrator role (a Windows built-in role) is the only role that should be allowed to install applications. This role should have no access to execute the election applications." Log into Windows as a System Administrator and launch each of the ES&S application. There are no system restrictions preventing the user from accessing each of the applications.	V.1:2.2.1.b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions. v.1:2.2.5.3 Third, the system shall be configured to execute only intended and necessary processes during the execution of election software. v.1:6.2.1.2. a Voting system vendors shall: Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access;	<b>MDN - 1.18.2009 - Revised hardening procedures provided with TDP Rev7a1 (1.18.2010). See Sec. 14, Appendix H -- Securing the Administrator Account.</b>	<b>Accept 2/22/10 KGW -- by review of Hardening Procedures EMS PC Unity 3.2.1.0 v.2.2 2/18/10 -- Verified System admin role may execute election specific software, but the system admin role utilizes a shared secret password so 2 election officials are responsible for these activities.</b>
82	10/12/09	Sjakileti & J. Garcia	Functional Defect	Closed	Server and Hardening Procedures for the EMS PC 9/18/09	Mapped "Z" drive is not visible to all users from the client PCs.  In Ch 2 section 7 it states "Closed Network - You must create users only for the Client PCs. Only the System Administrator should have access to the file database server. You must map each user to the file database on the network server." If the administrator only sets up the users on the client PC, the mapped drive cannot be seen by all users.	V.1:2.2.1.b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions. v.1:2.2.5.3 Third, the system shall be configured to execute only intended and necessary processes during the execution of election software.	<b>MDN - 1.18.2009 - Revised hardening procedures provided with TDP Rev7a1 (1.18.2010). See Sec. 4 for revised procedures for configuring a peer-to-peer network. See Sec. 17, Appendix K for procedure for configuring the EMS server share. See Sec 15.2 for mapping users to the share.</b>	<b>Accept 4/01/10 JG Verified in App. K of the Hardening Procedures EMS PC Unity v.3.2.1.0 3/10/10 Rev. 2.4 that the drive has been changed from "Z" to "Q" and all users can access the shared Q drive.</b>
83	10/13/09	J. Garcia	Functional Defect	Closed	AIMS 1.3.157	An export data validation error displays in AIMS when previewing ballots.  In Section 5.3.1 of the Information Management System Election Official's Guide it states, "Users of AIMS have the option of importing data directly from the ES&S Unity files. Doing this means that	V.1:2.2.1.b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.	<b>MDN - 3.8.2010 - Response dated 2.16 below is incorrect. Updated AIMS Election Officials Guide Provided with TDP Rev8a1. See Section 5.3.1, Note 10. - 02.17.2010</b>	<b>Accept 3/20/10 JG Verified AIMS Election Official's Guide 3/11/10 in Sec. 5.3.1 advises the users "Foreign language translations used with Str. Party / Party Preference</b>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>you do not have to reenter the election data, which has already been entered into Unity." Create an election in EDM with Spanish in each of the required fields. Import the AIS file from Unity, preview a ballot and at this point an error is displayed "export data validation process did not complete successfully. There was at least one language translation missing in the data. Would you like to view the data errors now?" The Spanish translation for the party does not import. It appears that all other Spanish translations are imported.</p>		<p><b>MDN - 2.16.2010</b>  Revised hardening procedures provided with TDP Rev7a1 (1.18.2010). See section 4 for updated hardening procedures. See Sec. 13.1.2 for securing election data folders.</p> <p><b>JML 10.28.2009:</b> The election in question includes Straight Party / Party Preference contests as well as English and Spanish languages. It was discovered that EDM does not include any foreign language translations in the LDF (Language Definition File) export for Straight Party / Party Preference. AIMS uses the encrypted version of this file (EDF) for translation details. AIMS provides a process for the user to add any missing translations (discovered via AIMS' Validation process). For this issue the Race Editor is used to Add Spanish translations not exported from EDM for Straight Party / Party Preference. Instructions for using the Race Editor can be found in Ch 10 of the AIMS Election Official's Guide. A NOTE will be added to Section 5.3.1 of the Information Management System Election Official's Guide</p>	<p>contests will not be included when importing into AIMS." The user must follow the instructions on missing translations steps.</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
								stating "Foreign language translations used with Straight Party / Party Preference contests will not be included in the EDM export for use with AIMS. AIMS validation process will identify any missing translations."		
84	10/13/09	Sjakileti & J. Garcia	Functional Defect	Closed	Windows Event Log 'Client/Server) Security TC	Windows Event Log is not recording actions on the shared "Z" drive.  Log on the Client as either a "Defineweuser" "Adminuser" or "Resultuser" go into the shared "Z" drive and modify two files (.CTN & .IFC). Log off and log on the Server as a Sysadmin. View the Windows Event Viewer from the server and it is only displaying the Windows login. Log back onto the Client as a Sysadmin and view the Windows Event Viewer. The Event viewer displays the Windows login and logoff; however, there is no evidence of modifying the two files.  <b>Rejected 11/2/2009 SJ:</b> Hardening procedures do not identify the folder names that need security tracking turned on  <b>Rejected 2/22/10 KGW:</b> The event log on the client does not detect access to the shared folder (Q). The event log on the file server detects the access, however it detects the access as "share" user. As everyone knows the password of the "share" user, there is no detection of the specific user access. This is related to Disc #86.	v. 1: 2.2.1.a Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability. v.1:2.2.5.3 ... operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object.	DWH - 3.8.2010 - Changed the Hardening Procedure - Appendix L from securing the Share account to creating Share User accounts. A unique share user accounts is now created for each remote user.  MDN - 1.18.2009 - Revised hardening procedures provided with TDP Rev7a1 (1.18.2010). See section 4 for updated hardening procedures. See Sec. 13.1.2 for securing election data folders..  JML 10.28.2009 "Hardening Procedures for the Election Management PC" document CH-12, "Turning Tracking On for a Folder" steps 4 - 6 detail the steps that enable the Event Log to record actions on " <u>any additional folder you want to monitor</u> ". The user would follow the same process on any folder on the "Z" drive.	Accept 04/09/10 JG KA: Tested and verified that when the Windows Event Log is active, logged into the shared Q drive (ES&S changed the Z drive to the Q drive) and a user modifies a file, the file modified and specific share user is displayed in the Windows Event Log. Appendix L of the "Hardening Procedures EMS PC Unity 3.2.1.0 3/10/10 REV 2.4" stipulates each user must be unique; accounts must never be shared.	Reject 2/22/10 KGW Reject 11/2/09 SJ
85	10/15/09	Sjakileti	Document Defect	Closed	CM- DS200 1.3.11.0c Source code change release summary	In the change release summary document the previous version from 3.2.0.0 is showing as 1.3.10.0b, but the previous version iBeta reviewed was	v.1:7.7To meet documentation requirements, vendors shall provide complete product documentation with	ES 10.29.2009 - Provided updated change release notes tracing source code	Accept 10/30/09 SJ: Updated documentation with correct version in	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
					document	1.3.10.0a.	each voting systems or components, as described Volume II, Section 2 for the TDP. This documentation shall include:: 12) System Change Notes.	versions 1.3.10.0a to 1.3.11.0c on 10.29.2009. File delivered via upload to the iBeta FTP server.	Change Release Summary Changes 1.3.10.0a to 1.3.11.0c
86	10/15/09	Sjakileti	Functional Defect	Closed	Peer-to-Peer Windows Event Log  Security TC	<p>Peer-to-Peer System Windows Event Log is not recording actions on the shared "Z" drive.</p> <p>Log on the system "Defineuser" "Adminuser" or "Resultuser" go into the shared "Z" drive and modify file (.IFC). Log off, Log back onto the same system as a Sysadmin and view the Windows Event Viewer. The Event viewer displays the user login and logoff, however, there is no evidence of modifying the file on shared Z drive</p> <p><b>Rejected 11/2/2009 SJ:</b> Hardening procedures does not identify the folder names that need security tracking turned on</p> <p><b>Rejected 2/22/10 KGW:</b> The event log on the client does not detect access to the shared folder (Q).The event log on the file server detects the access, however it detects the access as "share" user. As everyone knows the password of the "share" user, there is no detection of the specific user access.</p>	v.1: 2.2.1.a Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability. v.1:2.2.5.3 ... operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object. This ensures the accuracy and completeness of election data stored on the system. It also ensures the existence of an audit record of any person or process altering or deleting system data or election data.	<b>DWH - 3.8.2010 -</b> Changed the Hardening Procedure - Appendix L from securing the Share account to creating Share User accounts. A unique share user accounts is now created for each remote user. <b>MDN - 2.11.2010 -</b> See Sec. 13.1.2 for securing election data folders. <b>MDN - 1.18.2010 -</b> Revised hardening procedures provided with TDP Rev7a1 (1.18.2010) <b>JML 10.28.2009</b> "Hardening Procedures for the Election Management PC" document CH-12, "Turning Tracking On for a Folder" steps 4 - 6 detail the steps that enable the Event Log to record actions on "any additional folder you want to monitor". The user would follow the same process on any folder on the "Z" drive.	<b>Accept 03/18/10 JG</b> Hardening Procedures EMS PC Unity 3.2.1.0 3/10/10 was reviewed and the Share accounts were updated as specified in the procedure. Verified if a user on the client machine accesses the Q drive and attempts to modify a file in the Q drive, the server PC Windows Event log records the unique user and location.  <b>Reject 2/22/10 KGW</b> <b>Reject 11/2/09 SJ</b>
87	10/16/09	Sjakileti	Document Defect	Closed	CM- Build Document: DS200Firmware_BECI_v.1.3.11.0_2009.10.13.pdf	The previous DS200TOS post build image file name is wrong (the date showing as 05292009). The correct image file name from previous build -->DS200TOS_PostBuild_05302009.GHO	v.1: 8.5.a: The vendor shall establish such procedures and related conventions, providing a complete description of those procedures used to: a. Develop and maintain internally developed items;	<b>ES 10.29.2009 -</b> Revised documentation to correct the referenced build image file name. DS200Firmware_BECI_v.1.3.11.0_2009.10.21 provided with TDP Rev5a.	<b>Accept 11/2/09 SJ:</b> Verified the correct image name is listed in DS200 Firmware_BECI_v.1.3.11.0 1009.10.21.PDF

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							Testing and Certification Program Manual, v.1.0 Sec 5.5.1. Demonstrate that the software was built as described in the Technical Data Package.		
88	10/16/09	K. Wilson	Functional Defect	Closed	Windows Configuration Client Server Security TC	A non-administrative user can gain complete access booting from a BartPE CD, by passing the Windows Event Log.  On the Client-Server configuration, ERM laptop (E075 Dell PowerEdge) -- Using a non-admin BIOS login password the system booted from a BartPE CD in CD drive. The non-administrator had complete access to the entire system and by-passes the Windows Event Log. (See also #70 for Peer-to-Peer)	v.1:2.2.1.a & b a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.v.1:2.2.1.b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.	DWH - 1.28.2010 - Appendix C – Harden The System BIOS of the U3210_SSS08_Hardening Procedures document prevents booting the system from a CD.	Accept 4/7/10 JG KA Harden the PCs using "Hardening Procedures EMS PC Unity 3.2.1.0, 3/10/10, Rev 2.4" then verified that a non-administrative user could not boot or execute from the CD.
89	10/16/09	K. Wilson	Functional Defect	Closed	Windows Configuration Client Server Security TC step 3	The virus emulation program can be installed on the ERM server by a non-administrative user.  In the client-server network configuration the Results User, a non-administrator, was able to run and install a virus emulation program from a USB drive. The program was installed on the ERM laptop (test unit E075- Dell PowerEdge). (see #71 for peer-to-peer)	v.1:2.2.1.b b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions. c. Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met. v.1:2.2.4.1.f f. Protect against any attempt at improper data entry or retrieval v.1:2.2.5.3 Third, the system shall be configured to execute only intended and necessary processes during the execution of election software.	DWH - 1.28.2010 - The PreInstallNetwork.EXE and PreInstallNoNetwork.EXE scripts prevents a non-administrator from installing software.	Accept 4/7/10 JG KA Harden the PCs using "Hardening Procedures EMS PC Unity 3.2.1.0, 3/10/10, Rev 2.4" and the Preinstall-Network executable (scripts) than verified that a non-administrative user could not boot or execute a virus emulation program from the CD or USB.
90	10/16/09	K. Wilson	Functional Defect	Closed	Windows Configuration Client Server Security TC step 4b	A program can be executed on the ERM server by a non-administrative user without logging the event.  In the client-server network configuration	v.1:2.2.5.3 Second, operating system audit shall be enabled for all session openings and closings, for all connection	DWH - 1.28.2010 - The PreInstallNetwork.EXE and PreInstallNoNetwork.EXE scripts set the Audit	Accept 4/7/10 JG KA Harden the PCs using "Hardening Procedures EMS PC Unity 3.2.1.0, 3/10/10, Rev 2.4" and

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
						<p>the Results User, a non-administrator, was able to run an executable program (notepad.exe, iexplorer.exe) on the ERM server (test unit E075- Dell PowerEdge). A non-administrative user should not be able to run this program. Running of this program was not logged in the Windows Event Log. (see also #73 peer-to-peer)</p>	<p>openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object.</p> <p>v.1:2.2.5.3 Third, the system shall be configured to execute only intended and necessary processes during the execution of election software.</p>	<p>Policy to capture these events.</p>		<p>the PreInstall-Network executable (scripts) than verified that a non-administrative user could not boot or execute from the CD or USB. When attempting to execute an error is given and the error is also displayed in the Windows event log.</p>
91	10/19/09	k. Wilson/Sjakileti	Functional Defect	Closed	Client/server Windows Event Log  Security TC	<p><b>Client-Server Configuration:</b> Stopping the event log did not halt the election process</p> <p>Stopped the event log on the server, logged on as a result user on the ERM PC. The user was still able to access the files over the network from the server.</p> <p><b>Rejected 4/7/10 JG KA</b></p> <p>Access to the Q drive from the client workstation was not denied after disabling the Server Windows Event Log. Allowing user full functionality of the election process. The process was not halted.</p> <p><b>Rejected 4/22/10 CEC</b></p> <p>V.2:6.4.1 .b.2 identifies that the VSTL shall conduct tests to verify the correct operation of access controls, including: "Performing tests intended to bypass or otherwise defeat the resulting secure environment." The events logged on the Windows server deal with client users accessing the election file on the shared Q drive. This event is not captured in the Windows Event Log on the client.</p> <p>V.2:6.4 identifies that the VSTL "may conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities, employing test procedures approved by" the EAC. iBeta recommends submission of the test method to the EAC as we believe the test is valid. It has it has been used in prior certification testing of ES&amp;S and other</p>	<p>v.1:2.2.5.3 COTS General Purpose Computer System Requirements</p> <p>The system shall also be configured to halt election software processes upon the termination of any critical system process (such as system audit) during the execution of election software.</p>	<p>dwh – 20100503 - ES&amp;S has discussed the issue of simulating a failure of events being logged by the Event Log service with Microsoft's technical support. Following is a quote from Chandradeep Khalate Technical Lead , Directory Services, Microsoft Enterprise Platforms Support; "I also had a discussion regarding this with my Seniors. For the System to determine whether the Security Logs are full the Event Log Service has to be running. If the Service is not Running it will not work." Based on Microsoft's response and the ES&amp;S hardening configuration, a separate document is being provided which lists the steps that should be followed when attempting to simulate the failure of events being logged by the Event Log service running on the server. Document provided on</p>	<p><b>Accept 5/10/10 JG KGW</b></p> <p>Verified that if the server is configured with the Windows Event Log set to record, disabling the log will result in a system crash of the server. The active client user loses connection to the election database on the server Q drive. The applications on the client will not run without connection to the Q drive.</p> <p><b>Reject 4/7/10 JG KA</b></p> <p><b>Reject 4/22/10 CEC</b></p>	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						manufacturers. In Unity 3.2.1.0 this method of disabling the audit log demonstrated that the Log Monitor application successfully halted election software processes in the Stand-alone PC, Peer-to-Peer PCs and Windows 2003 Client.		20100504 via FTP under the folder titled "U3210_DISC91_TEST."  <b>SMP - 4.21.10</b> - This discrepancy was the direct result of a series of intentional actions performed by the VSTL tester to alter and operate the ES&S system in an improper and unauthorized configuration. The configuration settings for the ES&S EMS environments are provided in self-executing scripts executed only by the System Administrator during the installation and hardening process. These are a blended configuration based on National Institute of Standards (NIST), Center for Internet Security (CIS), and Microsoft recommendations and prescribed in the ES&S Hardening Procedures, Election Management System PC, Unity 3.2.1.0 procedures. Any change in recommended settings is a deviation from the ES&S' federally certified EMS PC configuration. In accordance with v.1:8.7.2 Functional Configuration Audit, "the FCA is conducted by the ITA to verify that the system performs all the functions described in	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							<p><i>the system documentation." This is an invalid and inappropriate test procedure. As further comment, in the Client-Server configuration as tested, there are no applications running on the data server. All EMS applications are running on the client PC's with full protection preventing them from operating upon the termination of any critical system process (such as system audit) during the execution of election software, therefore satisfying the intent of v.1:2.2.5.3 requiring the termination of those critical processes. In the ES&amp;S system, the critical EMS activities are all logged and monitored on the local event log regardless of the physical location of the data being accessed or updated. The only way data shared by the file server can be changed is either by intentional manipulation of the hardened environment (as was done in this case) or by the EMS applications running on the clients. In the event a System Administrator intentionally disables the data server Windows Event Log and intentionally reboots the system, all of the SA's</i></p>		

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								<p>actions are recorded in the server's log.</p> <p><b>DWH - 1.28.2010-</b></p> <p>Stopping the Event Log on the server will cause the Server to Blue Screen i.e. fail.</p> <p>Stopping Event Log on the Server will not prevent the applications from running on the Client. The fact the Server has failed would prevent the Client from accessing the Server shared folder.</p>	
92	10/19/09	K. Wilson/Sj akileti	Functional Defect	Closed	Peer-to- peer Windows Configuration Security TC	<p>In the peer-to- peer configuration the Resultuser logged into ERM was not able to access the shared Z folder,</p> <p>When selecting the Z drive in Miscellaneous-&gt; Change Control File, a message indicates the network drive does not exist. This message occurs regardless of whether the M100DEMO election or other elections present in the shared Z:\elecdata folder are chosen.</p>	<p>v.1:6.5.5: Shared Operating Environment: Systems that use a shared operating environment shall:</p> <ul style="list-style-type: none"> <li>a. Use security procedures and logging records to control access to system functions;</li> <li>d. Have capabilities in place to control the flow of information, precluding data leakage through shared system resources.</li> </ul>	<p><b>DWH -1.28.2010</b> - Will need additional information on this issue. It is possible that the share was not properly mapped using Explore   Tools   Map Network Drive.</p>	<p><b>Accept 02/19/10 JG KA</b></p> <p>No longer a Z drive. Now mapping to a shared Q drive.</p> <p>Verified the P2P ERM Client PC could map to the Shared Q drive without error (Hardening Procedure EMS Unity 3.2.1.0 v.2.2 2/18/10)</p>
93	10/20/09	K. Wilson	Functional Defect	Closed	Client Server Windows Configuration (step 4a) Event logging Security TC	<p>An ERM voting application file can be external modified and restored to without audit logging of the relevant events.</p> <p>The identical results to the #72 (p2p) were observed in the client-server network with the following workstations and servers: Ballot Prep, ERM, and Win2K3 Server. The windows security event log did not contain any events associated with access to the file.</p>	<p>v.1:2.2.1.a a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability</p> <p>v.1:2.2.5.3 Second, operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of</p>	<p><b>DWH - 1.28.2010 - Appendix G – Secure the EMS Server/Workstation of the U3210_SSS08_Hardening Procedures</b> document turns auditing on folders containing election data.</p>	<p><b>Accept 4/7/10 JG KA</b></p> <p>Harden the PCs using "Hardening Procedures EMS PC Unity 3.2.1.0, 3/10/10, Rev 2.4" and verified when a non admin and/or an admin user modifies a result file "DAT" it is logged in the Windows event log.</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
94	10/20/09	K. Wilson	Functional Defect	Closed	Windows Configuration (client/server) Security TC	On all tested machines (p2p & client-server) the account lockout policy is set to 10 tries, 15 minute lockout (in the local security settings, Account Policies, Account Lockout Policy). However the machines actually lock out after 5 tries for duration of 1 minute. Reproducible on four test platforms (iBeta inventory # E052, E079, E075, & E077).	v.1:6.2.1.1.d ... the vendor shall provide a description of recommended policies for: Effective password management.	DWH - 1.28.2010 - This observation is standard Windows XP behavior. The PreInstallNetwork.EXE and PreInstallNoNetwork.EXE scripts now set the limit for unsuccessful attempt to 5 tries.	Accept 4/7/10 JG KA Harden the PCs using "Hardening Procedures EMS PC Unity 3.2.1.0, 3/10/10, Rev 2.4" and the PreInstall-Network executable (scripts) than verified that after 5 tries the user was locked out. Each of the attempts and the "Account Lock out" message were logged in the Windows event log.
95	10/21/09	J. Garcia	Document Defect	Closed	M100 SMM FW 5.4.0.0 H Ver. 1.3	Inconsistencies between the M100 SMM and SOP documents.  Ch 1 pg 4 of the M100 Maintenance Manual states, "PC Cards: Battery backed PC cards that store the scanner's election definition and ballot count. The standard memory capacity for Model 100 PC Cards is 256k but larger sizes are available. Recommended Quantity: 1 per scanner". However the smallest PC card in the Operations Manual states " Use PC cards with a memory capacity of 512KB (kilobytes)."	v.2:2.9.4 Vendors shall provide detailed documentation of parts and materials needed to operate and maintain the system. Additional requirements apply for paper-based systems.	10.29.2009- DJZ M100 SMM - Updated the specified PCMCIA card size: (Cards of 512k or 4MB are available for use.)	Accept 11/4/09 SJ: Verified M100 Sys Maint. Manual FW v.5.4.0.0 HW 1.3 10/29/09 documents the correct PC card size in ES&S
96	10/21/09	J. Garcia	Document Defect	Closed	ES&S M100 SOP FV 5.4.0.0 H Rev 1.3	Ch 5 pg 28 of the System Operations document states "The Model 100's multi-sheet sensor prevents multiple ballots from passing through the tabulator's read area at the same time. Test the multi-sheet sensor before Election Day to make sure that your tabulator does not accept multiple ballots.". This is a pre-election maintenance procedure which is not performed in the polling place.	v.2:2.9.2.1 a. All required and recommended preventive maintenance tasks, including software tasks , database performance and turning.	10.29.2009 DJZ -- Model 100 SOP: Moved the procedure for testing the Multi-Sheet Sensor from the pre-election tasks section to Ch 8, "Maintaining the Counter," to clearly identify this task as a maintenance level procedure.	Accept 11/4/09 SJ: Maint. Manual FW v.5.4.0.0 HW 1.3 10/29/09 verified moving the section testing the Multi-sheet sensor from election day task list to pre-election maintenance list.
97	10/22/09	Sjakileti	Document Defect	Closed	AutoMARK AIMS SW Compilation Instructions Release date 9/17/09	In section 2. Load the AIMS Source section, under b, it is documented as repeat the previous step with 'AIMS' 'VAT' PACKAGE zip file. The build is only for the AIMS build. There is no VAT build.	v.1: 8.5.a :The vendor shall establish such procedures and related conventions, providing a complete description of those procedures used to: a. Develop and maintain	10.28.2009 RF -- Revised the AutoMARK AIMS Software Compilation Instructions (Rev.2) to remove this reference. Delivered with TDP Rev5a1.	Accept 11/2/09 SJ: Verified AutoMARK AIMS Software Compilation Instructions Rev.2 contain the correct build package name

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							<i>internally developed items;</i> <i>EAC Voting System Testing and Certification Program Manual, v.1.0 Sec 5.5.1. Demonstrate that the software was built as described in the Technical Data Package.</i>		
98	10/22/09	K. Wilson	Informational	Closed	Server and Hardening Procedures for the EMS PC 9/18/09	<p>Section 5.2 Configure the LAN - Entering Static IP Addresses - item 4 the static IP address as shown below. -- the figure shows a subnet mask of 255.255.255.240 which would allow only 14 addresses on the subnet. While this may be sufficient for the peer-to-peer configuration, it may not be sufficient for the client-server configuration. Likewise in section 5.2 paragraph 1 the range of IP addresses includes x.x.x.15. However x.x.x.15 is the broadcast address with the mask given above.</p> <p><b>02/03/10 KA Rejected:</b> Appendix J still shows a subnet mask of 255.255.255.240, only allowing 14 addresses on the subnet.</p>	v.1:8.7.1.h.2) Confirming whether the system documentation matches the corresponding system components.	<p><b>DWH - 2.182010 -</b> ES&amp;S feels the XP limit of 10 workstations is more than sufficient and the current subnet mask supports this number of address . The table in the Appendix J of the Hardening document outlines how these 16 address should be used.</p> <p><b>MDN - 1.18.2009 -</b> Revised hardening procedures provided with TDP Rev7a1 (1.18.2010). See Sec. 16, Appendix J. ES&amp;S is currently testing listed settings for Win2003 server configuration.</p>	<p><b>Accept 02/19/10 JG KA</b> Verified the documented system set up in the "Hardening Procedures for the EMS PC" v.2.2 02/18/10 matches the system set up. Also verified 10.0.0.15 is Reserved.</p> <p><b>Reject 02/03/10 KA.</b></p>
99	10/22/09	K. Wilson	Functional Defect	Closed	Security Test - Client Server Windows Configuration (step 4c)	<p>Launching of ERM, EDM was not logged on the client.</p> <p>Identical to #74 (p2p) for the client server: In the client-server network configuration the Results User, a non-administrator, launched ERM. Likewise the Define User, a non-administrator launched EDM, or HPM. Launch of the program was not logged in the Windows Event Log on the client.</p>	v.1:2.2.5.3 Second, operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object.	<p><b>DWH - 01/28/10 - Appendix I - Creating User Accounts of the U3210_SSS08_Hardening Procedures</b></p> <p>document allows users to only run applications based on the pre-defined group they are a member of i.e. ElectAdmin, ElectDefine, or ElectResult.</p>	<p><b>Accept 04/08/10 KA &amp; JG.</b> Verified using "Hardening Procedures EMS PC Unity 3.2.1.0, 3/10/10, Rev 2.4" that launching of ERM or EDM by a non administrative user is logged in the Windows Event Log on the client workstation. Logged in as elect-result1, a non-administrator, launched ERM. and logged in as elect-define1 , a non-administrator, and launched EDM, Launch of the</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
									programs was logged in the Windows Event Log on the client.
100	10/26/09	K. Wilson	Document Defect	Closed	Hardening Procedures for the EMS PC 10/16/09	Pg 28 Configure the File Server. Option 1 states to create and share the ESS\electdata folder on the Server as the Z: drive for other PC's on the network in the peer-to-peer case. However Option 2 does not make these statements. This omission leads to confusion in the configuration of the Windows 2003 Server system during testing.	v.2:2.6.4 The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure software (including firmware) installation to meet the specific requirements of Volume I, Section 6.4 of the Standards. This information shall address software installation for all system components.	<b>10.29.2009 BB --</b> Revised Section 5.1 of the Hardening Procedures for the Election Management PC(U3210_SSS08_Hardening Procedures) to include the instruction for setting up the server drive included under option 1 within the option 2 instruction as well.	Accept 11/2/09 SJ: Updated documentation with steps for Windows 2003 server based network in Hardening Procedures for the Election Management System PC Oct 30,2009
101	10/27/09	S. Eaton	Document Defect	Closed	AutoMARK Information Management System Election Official's Guide 9/25/09	The documentation states the user must manually uninstall the AIMS ESS.DLL and Microsoft's SQL Server Desktop Engine however, uninstalling "AIMS for ES&S 1.3" program will automatically uninstall the applications.  After uninstalling "AIMS for ES&S 1.3" from the Add/Remove program the documentation states, "(pg 32 #3 Uninstall AIMS ESS.DLL) The Windows Installer Cleanup Utility is required to uninstall the AIMS ESS.DLL." and "(pg 38 #4 UNINSTALL MICROSOFT SQL SERVER DESKTOP ENGINE) 1. Click Start, click Control Panel, and then click Add or Remove Programs. 2. When the currently installed programs appear, click Microsoft SQL Server Desktop Engine (AIMS_SQLS)." However, after uninstalling "AIMS for ES&S 1.3" and refreshing the Add/Remove Program window the AIMS ESS.DLL and MICROSOFT SQL SERVER DESKTOP ENGINE no longer display.	v.2:2.6.4 The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure software (including firmware) installation to meet the specific requirements of Volume I, Section 6.4 of the Standards. This information shall address software installation for all system components.	<b>MDN - 2.11.2010 -</b> Revised Section 3.3. to remove instructions for separately uninstalling AIMS ESS.dll and MICROSOFT SQL SERVER DESKTOP ENGINE. Uninstalling AIMS using the standard Windows Add/Remove Programs procedure now removes these elements as well.	Accept 02/16/10 SLE: Verified in the AIMS Election Official's Guide v.18.0 11/24/09 document that the instructions to separately uninstalling AIMS ESS.dll and MICROSOFT SQL SERVER DESKTOP ENGINE were removed.
102	10/27/09	S. Eaton	Document Defect	Closed	AutoMARK Information Management System Election Official's Guide 9/25/09	In section 3.3 (pg 29) a NOTE is displayed "NOTE: Do NOT save the backup files to the AIMS folder – save them to a different location, because the AIMS folder will be deleted." however in	v.2:2.8.5 Operating Procedures The vendor shall provide documentation of system operating procedures that	<b>MDN - 1.18.2009 -</b> File delivered with TDP Rev7 (1.12.2010). See Sec. 13.1. Changes described below.	Accept 01/29/10 KA - Verified in the AIMS 3010 sect05 Election Officials guide that a warning note has been

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						section 13.1 "Backing up/Restoring the AIMS Database" there is no NOTE/warning reminding the user not to save a backup file to the AIMS folder.	meets the following requirements: a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation.	11.22.2009 MDN -- Added a warning to AIMS 3010 Sect05 Election Officials Guide AQS-13-5001-208-R 07 Section 13.1, "Backing up/Restoring the AIMS Database," instructing the user to avoid backing up to the default, AIMS folder prior to uninstalling/re-installing AIMS	added to section 13.1 concerning avoiding use of the AIMS folder. 11/24/09 SLE - review is pending document delivery
103	11/03/09	K. Wilson	Document Defect	Closed	System Security Spec Ver. Rel. 3.2.1.0 9/25/09 (SSS) ES&S System Functionality Description M100 Unity v. 3.2.1.0 (SFD) System Overview Unity v. 3.2.1.0 10/21/09 (OVR)	Documentation does not address ERM read only access to incomplete election returns.  The procedures given in the SFD section 1.1.5.3 indicate that ERM has the capability to access incomplete election returns prior to completion of the official count. None of the cited documents provide the jurisdictions with the capability to restrict persons, whose only authorized access is to query the reporting of incomplete election returns, from having the capability to write-back to the database (6.5.6.b.2). In the figures 1.4.2 and 1.4.3 of OVR it shows a networked ERM workstation with a projector displaying incomplete election returns.  <u>4/13/10 JG Re-open:</u> ES&S is removing HPM and ERM Manager (Security Procedures for multiple users) per disc. #136, as such this invalidates the prior acceptance : Accepted 3/15/10 JG Unity 3.2.1.0-SFD M100 dated: 3/09/10 Section 1.1.5.3- Verified M100 Incomplete Election Returns and administrative procedures required to restrict query of incomplete returns. Update verified in Regression test.  <u>4/22/10 CEC Reject:</u> iBeta agrees that this issue does not involve telecommunication or data transmission.	v.1:6.5.6 If the voting system provides access to incomplete election returns and interactive inquiries before the completion of the official count, the system shall: ... b. Use voting system software and its security environment designed such that data accessible to interactive queries resides in an external file, or database, that is created and maintained by the elections software under the restrictions applying to any other output report, namely, that: 1) The output file or database has no provision for write-access back to the system. 2) Persons whose only authorized access is to the file or database are denied write-access, both to the file or database, and to the system.	MDN - 20100607 -- ERM Manager has been re-instated in Election Reporting Manager. Updated documentation submitted with TDP Rev10 06.07.2010 <b>SMP - 04.21.10 -</b> ES&S wishes to resubmit Gary Weber's 03.25.10 comments below. v.1:6.5.6 was written to address four specific areas pertaining to telecommunications and data transmission: (1) access control for telecommunications capabilities, (2) data integrity, (3) protection and detection of data interception, and (4) protection against external threats to which commercial products used by a voting system may be susceptible. The Unity 3.2.1.0 release does not support any form of telecommunications or data transmission outside of its hardened and closed network and stand-alone	Accept 09/07/10 SAB Verified that information added to document for #173 below relates to this discrepancy as well. Once the control files are copied to server, then it is possible to apply the steps as defined on pg 60-63 which sets the ERM security. Confirmed a new note has been added to change the default drive to the server drive (if needed) under step #5. Confirmed with testing that security does exist as now described in the documentation for ERM (SOP).  <b>Reject 4/22/10 CEC</b>  <b>Reopen 4/13/10 JG</b>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p><i>It only deals only with restrictions to query/write access within the ERM network. (i.e. only v.1:6.5.6.b) It is iBeta's understanding that the "Results Display Workstation" identified in the Peer-to-Peer (figures 1.4.2) and Windows 2003 Server (figure 1.4.3) of the System Overview dated 4/16/10 are for the purpose of providing a public display of incomplete election returns prior to the completion of the official count. ERM previously met v.1:6.5.6.b with an application level read-only access control. When ES&amp;S removed the ERM application specific access controls and replaced them with the Windows level access controls they did not provide a query/read-only access control to ERM. Users with access to ERM have query and write-access. In ES&amp;S' v.1:6.5.6.b response they described a scenario that is not represented in the either the Overview figures 1.4.2 and 1.4.3 or the SFD section 1.1.5.3 description of ERM user access controls. (In the Overview figures the "Results Display Workstation" is connected to an ERM network. The SFD identifies that there are ERM application user controls.) The ES&amp;S response to v.1:6.5.6.b would comply if this documentation reflected the scenario described.</i></p>		<p><i>environments. Only fully authorized ERM user determined by the Election Administrator and established by the System Administrator with ElectResult rights have access to the application (ERM) required to read in results and release report election results. If further discussion is determined to be necessary, ES&amp;S recommends seeking clarification from the EAC for final determination.</i></p> <p><b>GLW - 03.25.10 - Vol. 1.</b>  <i>Section 6.5 deals specifically with Telecommunications and Data Transmission – even in the strictest sense we have neither in our 3.2.1.0 voting system. We do not provide access to or allow interactive inquiries against the ERM results database other than by the internal ERM users defined by and allowed for by the System Administrator. This internal access by authorized ERM users does not involve Telecommunications or Data Transmission in either a stand-alone, peer-to-peer or Server based LAN configuration.</i></p> <p><i>Movement of data within a closed LAN is not</i></p>	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							<p>telecommunications or data transmission.</p> <p>6.5.6 is contemplating a voting system that may allow "outside" access to either the official ERM results database or to a secondary, external file created from the official results database within the same LAN environment. Unity 3.2.1.0 does not provide for such access to either the official results or a secondary, external file on the voting system closed LAN. 6.5.6 (a) specifically addresses central count and precinct count equipment, not the EMS Results Reporting Module.</p> <p>6.5.6 (b) provides additional requirements for voting systems that provide a secondary or external file of election results for purposes of interactive queries – we do not provide this capability in 3.2.1.0.</p> <p>It is common practice for ERM users to periodically create on election night one the results export file formats available in ERM and then sneaker net these static, flat files representing the current results reported from all tabulators to a totally separate computer not part of the certified voting system for purposes of publishing</p>		

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								results to external resources. <b>SLM 03.09.10 – ES&amp;S'</b> M100 SFD – Section 1.1.5.3 explains the incomplete election returns functionality in working in conjunction with the ERM	
104	11/16/09	K. Wilson	Document Defect	Closed	Unity 3.2.1.0 System Security Spec (9/25/09), M100 System Functionality Description (10/20/09)	<p>Neither the System Security Specification (SSS) or the System Functionality Description (SFD) for Unity 3.2.1.0 describes sufficiently detailed procedures for application and inspection of the ES&amp;S provided tamper evident seals. Issues of specific concern include:</p> <ul style="list-style-type: none"> <li>1. Wire seals that are not wound snuggly, so that it can be cut and be re-fed into the spool without detection.</li> <li>2. Destructive disassembly of two wire seals (one by drilling out the inside piece, one by cracking open the outside piece) and then reassembled to make a new seal with a correct number, most likely on the outer piece tab.</li> <li>3. A blue all-plastic seal that is not wrapped snuggly which can be cut and reinserted into the lock without documented techniques for detection.</li> </ul> <p><b>2/17/10 KA &amp; JG Reject</b> The ES&amp;S System Security Specification Ver. Release 3.2.1.0 dated 2/12/10 in Ch 2 it states the user can or should use tamper evident seals however does not require the use of tamper evident seals.</p>	v.1: 2.2.1.a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability	<b>BB 02.12.2010 SSS - Added M100 Security Seals section to Ch 2, "Appendix - Model 100 Security Seals."</b>	<b>Accept 2/17/10 JG KA</b> Verified System Security Spec Ver. Rel. 3.2.1.0 2/17/10 enforces the use of tamper evident seals and the enforcement of the PCMCIA latch to be securely tightened. <b>Reject 02/17/10 KA &amp; JG</b>
105	11/30/09	K. Wilson	Functional Defect	Closed	Unity 3.2.1.0 System Functionality Description M100 11/23/09 [SFD]	<p>Seal delivered for testing do not include all ES&amp;S product offerings.</p> <p>The SFD in section 1.1.1 refers to the ES&amp;S website which in turn has 16 types of seals. Not all of these were delivered for testing and yet the documentation suggests that all of them are valid for the 3.2.1.0 certification. Items listed which were not provided include: 00555-xx, 00553-00, 00554-00, PS-BBS, 00556-01, RISBL, RISB, E113, RINS, RINS1,</p>	v.1: 2.2.1.a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability	<b>SLM 05.03.10 - Modified Section 1.1.1 of the M100 SFD.</b> <b>SLM 04.29.10 - Modified Section 1.1.1 of the M100 SFD to show some of the security seals that could be used on the M100 and ballot box.</b>	<b>Accept 5/04/10 JG KA</b> Verified ES&S SFD M100 Ver. 10.0 5/03/10 Section 1.1.1 list of the seals ES&S offers to secure the M100 and ballot box matches the seals provided for testing.

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						RIFS1, RIFS2 . (iBeta has received & tested: 86022, 6024, 6320000, 00561-xx) <b>3/15/10 JG Reject</b> ES&S provided seals however, iBeta did not receive the following: RIFS1, RIFS2, 632000, 00561-xx. iBeta did receive 2 seals that are not documented in the SFD or on the web site listing all of the seals. (Manfr: A Rifkin Co.-plastic, no part #.)		SLM - 03.09.10 - Changed the M100 SFD - Section 1.1.1 to list the part numbers of those seals that are to be used with the M100.	Reject 03/15/10 JG
106	01/07/10	J. Garcia	Document Defect	Closed	M100 SOP F V 5.4.0.0 Rev.1.3 10/29/09	The SOP does not provide any information on how to calibrate counterfeit sensors on the M100.  M100 Ops documentation does not provide the user with instructions as to how to calibrate the counterfeit sensor M100 scanner. (Identified in Discrepancy #7 response)  <b>Reject 02/17/10 JG KA</b> ES&S' 2/11/10 response contradicts the M100 SMM (FW v. 5.4.3.0 HW v. 1.3 2/12/10) that states "ES&S will train county personnel to perform corrective maintenance procedures on the M100. Trained to perform corrective maintenance will also be responsible for preventive maintenance and pre-election testing." If ES&S trains personnel to perform maintenance procedures the SMM documentation needs to reflect the types of maintenance performed.	v.2: 2.8.5a  The vendor shall provide documentation of system optioning procedures: a. Provide a detailed description of procedures required to initiate, control, and verify proper system operation.	<b>SLM - 03.09.10</b> ES&S withdraws the previous statement of 2.11.10. There is no calibration setting on the M100 for counterfeit detection.  <b>MDN - 2.11.2010</b> - Model 100 counterfeit ballot sensors are factory calibrated and re-adjusted only by an ES&S technician during preventative or corrective maintenance. ES&S does not document this process for an end-user because calibration is a physical	<b>3/12/10 Accept CEC</b> ES&S has clarified that there is no calibration setting on the M100 in their response to #7 and 106. The issue is closed because there is no process to document.  <b>Reject 02/17/10 KA JG</b>
107	01/07/10	J. Garcia	Functional Defect	Closed	HPM - writing a PCMCIA card with the OMNI-Parallel Drive	Selecting the "OMNI-Parallel Drive" option does not permit the user to write to the PCMCIA card or provide the action required to write the card  While attempting to load the election data to the PCMCIA Card (M100 media) using the "OMNI-Parallel Drive" an error is displayed "Unable to access Omni Drive: OMNI97". The user has 3 options to select. 1) Abort to close the window, 2) Retry to make another attempt and 3) Ignore. Selection of Retry displays the same error and selecting Ignore displays the message "There is nothing left to do".	v.1: 2.3.3 All systems shall provide a means of installing ballot and programs on each piece of polling place ... equipment ...  v.1: 2.2.5.2.e The message cue for all systems shall clearly state the action to be performed in the event that operator response is required.	<b>DJZ 02.12.2010</b> HPM SOP - Updated Warning messages and resolutions in Ch 36.  <b>EBD 02.12.2010</b> HPM SFD - Updated warning messages under section 1.1.5.1.b  <b>SLM 02.11.2010</b> - This issue is resolved in the new HPM version 5.7.2.0.	<b>Accept 2/23/10 JG KA</b> Verified the ES&S HPM SOP Ver. Rel. 5.7.2.0 dated 2/12/10 clarifies the use of the settings with the different hardware configurations (Note: Functional testing with the OMNI-Parallel Drive is performed in the Regression TC)

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
						Neither option results in the election being written to the PCMCIA card. Nor do they provide a clear message as to what the users action is to correct the problem.				
108	01/19/10	K. Wilson	Document Defect	Closed	Hardening Procedures EMS PC Unity 3.2.1.0 1/18/10	<p>Inconsistent statements regarding the handling of OS patches</p> <p>Section 6.1 states that "Changes to the system patch level would be a deviation from the approved/certified configuration." This statement, in terms of the OS patches, is contradicted by the procedures described in Section 10 (Appendix D). During the procedures in Appendix D, specifically 10.2.2-3.b.i, the most recent updates to the Windows Operating Systems and COTS will be downloaded. Therefore the OS patch level from one installation to another will not be identical unless all jurisdictions were to download the patches at the same time.</p> <p><b>2/10/10 Reject CE Coggins</b> - The VSTL has neither the capability nor the commercial authority to distribute Windows OS patches. The VSTL documents the list of patches and updates applied as a record of the test environment. This information is available to ES&amp;S.</p> <p><b>3/8/10 Reject CE Coggins</b> - Hardening Procedure v.2.2 2/18/10 -The first paragraph in section D contains the direction to obtain the most recent updates from Microsoft. While we understand that some jurisdictions do not require EAC certification the language is not sufficiently clear as to identify to whom the first paragraph is applicable and to whom the second paragraph is applicable. As currently written it appears that the two paragraphs are contradictory.</p>	v.2.2.5.5.2 The vendor shall identify the compilers or assemblers used in the generation of executable code, and describe the operating system or system monitor.	<p><b>DWH – 03.10.2010</b> – Updated the first three paragraphs of Appendix D to clarify the procedure.</p> <p><b>DWH – 02.18.2010</b> – See Appendix D of the latest submission of the Hardening document. The WSUS Offline Update is free software and is licensed under the GPL 3, or the GNU General Public License Version 3. This, in condensed terms, means that the program is completely free, and that it can be freely redistributed and modified as the source code of the project is readily available to whoever wishes to obtain it as per the terms and conditions of the GPL 3 End User License Agreement (EULA). It is also based on freely redistributable updates and utilities provided by the Microsoft Corporation that are downloaded from their main support website. However, the Hardening document has been changed to read as follows: The update applied during certification should be used and can be</p>	<p><b>Accept 03/11/10 KA</b> Verified in Hardening Procedures EMS PC Unity 3.2.1.0 03/11/10 v.2.4 that language identifies to whom the action is applicable. A distinction is made to updates that are for certified systems.</p> <p><b>3/8/10 Reject CEC</b></p> <p><b>2/10/10 Reject CEC</b></p>	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								obtained from either ES&S or the State based on the jurisdiction's policies. <b>DWH - 02/05/10 -</b> Added the following statement to Appendix D. The update applied during certification should be used and can be obtained from the VSTL. However, should the jurisdiction choose to install a more recent update, only a qualified system administrator, when specifically directed to do so by the Election Administration authority, should perform this update.	
109	01/19/10	K. Austin	Informational	Closed	Table of Contents U3210_SFD00_HPM v.3.0 & U3210_SDS00_DS200	The Table of Contents in the following documents in the TDP display Error! Bookmark not defined: System Functionality Description HPM Unity v. 3.2.1.0 (v.3.0) DS200 System ES&S Software Design Specifications DS200 Unity v. 3.2.1.0 (v.3.0)		MDN - 2.11.2010 - Reprinted U3210_SDS00_DS200 (Software Design and Specification for the DS200) for TDP Rev8 delivered 2.12.2010. Document Revision remains Rev 3.0. No content changes. U3210_SFD00_HPM replaced in TDP Rev8 due to product updates. TOC u	Accept 02/16/10 SLE: Verified in SDS DS200 v3.0 12/22/09 and SFD HPM v4.0 02/08/10 that the Tables of Contents do not display a bookmark error
110	01/20/10	J. Garcia	Functional Defect	Closed	DS200 Plastic Ballot Box (HW Rev 1.2 and 1.3)	The carrying case part number labels are missing from the DS200 Plastic Ballot Boxes.  The DS200 Plastic Ballot Box is made up of a ballot bin paired with a carrying case. The bin and carrying case have unique part numbers. The carrying case for the DS200 Plastic Ballot Box hardware Rev. 1.2 does not contain a nameplate or label for part number "94099". Hardware Rev 1.3 carrying case is missing a nameplate or label for part	v.1: 3.4.6.a All voting systems shall: Identify all devices by means of a permanently affixed nameplate or label containing the name of the manufacturer or vendor, the name of the device, its part or model number, its revision letter, its serial number, and if applicable, its power requirements;	ESS supplied part number labels for the Carrying cases ECO 000618 was previously submitted	Accept 2/10/10 CEC Verified ECO000618 addresses labels for separate part numbers for the DS200 case & bin 2/5/10 KA. Received and applied part number labels to the DS200 Carrying Cases.

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
111	01/22/10	K. Austin	Informational	Closed	System Limitations Unity v. 3.2.1.0 1/8/10	The Introduction does not reference the M100 number "94051". While the document provides system limits for the M100 , it is missing from the systems listed in the Introduction.		MDN - 2.11.2010 - Removed product specific verbiage from the introductory narrative.	Accept 02/16/10 SLE: Verified System Limitations v7.0 01/28/10 removed all product-specific verbiage from the introduction.
112	01/19/10	K. Wilson	Document Defect	Closed	Hardening Procedures EMS PC Unity 3.2.1.0 1/18/10	Instruction to disable ports prevents function as designed in networked peer-to-peer and server configurations. Sec. 9.1.g states "If supported, disable all network ports, wireless, and landline modems" Appendix C is utilized by all installations, both networked and non-networked, so disabling network ports for the networked systems prevents the system from functioning as designed.	v. 1:2.2.1.a a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability	DWH - 02/05/10 - Modified/Added the following statements: If supported, disable all wireless and landline modems. If supported and you are setting up a non-networked environment, disable all network ports.	Accept 2/9/10 KA. Change has been made in the Hardening Procedure 2/8/10
113	01/22/10	K. Wilson	Document Defect	Closed	System Change Notes for M100 v.5.4.2.0 & ERM v.7.5.6.0	Change notes were not submitted System Change Notes describing the functional modifications of M100 v.5.4.2.0 and ERM v.7.5.6.0 from the previously tested revisions 5.4.2.1 and 7.5.5.0 were not provided	v. 1:7.7 Vendors are required to produce documentation to support the development and formal testing of voting systems ... a. Be sufficient to serve the needs of the ITA, voters, election officials, and maintenance technicians; ... c. Consist, at a minimum, of the following ... 12) System Change Notes	MDN - 2.18.2010 - Updated change notes to reflect current functionality of all products. Delivered with TDP Rev8a2.	Accept 02/24/10 JG Verified ES&S delivered the Unity 3.2.1.0 System Change Notes Rev 04
114	01/25/10	K. Austin	Document Defect	Closed	Unity 3.2.1.0 System Change Notes Rev 3.0	System change notes are missing details regarding the configuration, document changes and testing. This system change listings do not provide specific detail of the modifications made to the system configuration items. It does not provide detailed references to the sections of documents changed, nor reference the test plan and procedures executed by the ES&S to test the changes, the system, and test results. (The System Change Notes format submitted in this document is inconsistent with the format previously submitted in the 3.2.0.0 certification.)	v.2:2.13b A listing of the specific changes made, citing the specific system configuration items changed and providing detailed references to the sections of documentation changed v.2:2.13c The specific sections of the documentation that are changed (or complete revised documents, if more suitable to address a large number of changes) v.2:2.13d Documentation	MDN - 2.18.2010 - Updated change notes to point to documentation updated in response to system changes. Specific sections of documents changed are listed in the revision histories for individual documents. Also cross-referenced system test cases that relate to each change.	Accept 04/02/10 KA Verified the Unity 3.2.1.0 System Change Notes Rev 7.0 (no date) reference the documents updated, the test plans, and the format is consistent with previously submitted change notes

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							of the test plan and procedures executed by the vendor for testing the individual changes and the system as a whole, and records of test results.		
115	02/01/10	J. Garcia	Document Defect	Closed	M100 SOP FV. 5.4.2.0 HW Rev 1.3 1/8/10	<p>The M100 SOP states that the Firmware upgrade procedures are for a newer version of the M100.</p> <p>In Ch 4 (Install Model 100 Firmware) pg 15 it states "These instructions are for versions 5.0.0.0 and newer of the Model 100. Use a PCMCIA firmware update card to install new firmware on the Model 100." However, these instructions appear in the Unity 3.2.1.0 version.</p>	v.2.2.8.1  The vendor shall provide a summary of system operating functions and mode, in sufficient detail to permit understanding of the system's capabilities and constraints.	<b>DJZ 02.12.2010 M100 SOP</b> - Removed text referring to specific version.	<b>Accept 02/16/10 SLE:</b> Verified M100 SOP FW Ver. 5.4.3.0 HW Rev 1.3 02/12/10 removed references to 5.0.0.0 from Ch 4
116	02/02/10	J. Garcia	Document Defect	Closed	M100 SOP FV. 5.4.2.0 HW Rev 1.3 1/8/10	<p>The M100 SOP documentation does not identify the new feature of printing an audit log after the log has reached its capacity.</p> <p>A new feature allowing the user to either print or not print the audit log a full audit log is not documented in the ES&amp;S M100 System Operation Procedures document.</p>	v.2.2.8.5a  The vendor shall provide documentation of system operating procedures.... Provides a detailed description of procedures required to initiate, control and verify proper system operations.	<b>DJZ 02.12.2010 M100 SOP</b> - Added note in Ch 9: Reports the user can print or not print an audit log.	<b>Accept 02/16/10 SLE:</b> Verified M100 SOP FW v.5.4.3.0 HW Rev 1.3 2/12/10 Ch 9: Reports identifies that the user will be able to choose to print or not print the audit log after the log has reached its capacity".
117	02/04/10	K. Wilson	Document Defect	Closed	Hardening Procedures EMS PC Unity 3.2.1.0 January 18, 2010	<p>Audit is not enabled for alteration or deletion of any memory or file object.</p> <p>The procedures in Section 13.1.2 is only setting auditing for folders containing election data. It does not address other memory or file objects</p>	v.2: 2.2.5.3 Second, operating system audit shall be enabled ... for the alteration or deletion of any memory or file object.	<b>DWH - 2.18.2010</b> - See Appendix G in the latest submission of the Hardening document. Auditing has been changed from folder containing election data only to include the entire local hard drive.	<b>Accept 02/19/10 JG KA</b> Verified Hardening Procedure v.2.2 2/18/10 Appendix G section 13.2 sets auditing of the local drive (i.e. C :\.)
118	02/05/10	J. Garcia	Functional Defect	Closed	Accessing Election Data files using WordPad / Sec TC - Stand-alone Windows Config)	"WordPad" is inconsistently blocked. It is unclear, based upon the availability of "WordPad", if it is intended and necessary to execute the election software. Access is denied when selecting "Start/All Programs/ Accessories/WordPad". However a user can access "WordPad" by selecting a file and choosing to open it with "WordPad". Once the user has access to "WordPad" they can delete or edit the contents of the	v.2:2.2.5.3 Third, the system shall be configured to execute only intended and necessary processes during the execution of election software.	<b>DWH - 2.18.2010</b> - The ESSIM SOP will be updated to include "WordPad" as a required utility.  <b>MDN- 2.18.2010</b> - See ESSIM SOP Ch 4, "Install ES&S Image Manager," for the WordPad requirement. Document delivered	<b>Accept 02/19/10 JG KA</b> Verified the ESSIM SOP Ver. Rel. 7.7.1.0 2/12/10 now states "WordPad" is required for ESSIM Validation and Ballot Style reports and any modification using WordPad was logged in the Windows event

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
						election. In testing we deleted Precinct6 and its contents, saved the file and attempted to open HPM and go to the election. The HPM application gave a Cobol error when the election was selected. This confirmed that the Event Viewer (log) identified that the modification and the Cobol error were detected. If "WordPad" is an intended and necessary application then the detection meets the VSS. However, there is no documentation provide by ES&S that identifies "WordPad" as intended and necessary.		with TDP Rev8, 2.12.2010.	log.	
119	02/08/10	J. Garcia	Functional Defect	Closed	Windows Event Log testing of Log Monitor-Stand-alone (Re-enable audit logging -Sec TC Security tab)	Cannot Enable the Windows Event Log once it has been disabled.  On the Stand-alone configuration, In testing that the Log Monitor will prevent access to the EMS applications when the Windows Event Log is disabled, the "Sysadmin" user disabled the Windows Event log and restarted the PC. After validating all users could not access the EMS applications, the "Sysadmin" user enabled the Windows Event log, restart the PC and attempted to open ES&S applications. The applications would not open and the system continued to act as though the Windows Event log was still disabled. Logged off and attempted to log in as non admin users. The users were not allowed access.	v.1:2.2.5.3  Second, operating system audit shall be enabled ... for the alteration or deletion of any memory or file object.  Third, the system shall be configured to execute only intended and necessary processes during the execution of election software.	DWH - 2.18.2010 - See the latest submission of the Hardening document. Changed section title from "Installing Essential Updates" to "System Maintenance and Support" and added procedures on recovering from a blue screen if event logs become corrupt or the event log service is disabled as in your test case.	Accept 4/7/10 JG KA Verified in all instances where the Windows Event Log was corrupted and the blue screen appeared a user was able to restore access (following the hardening procedures listed below). If the blue screen is not generated the issue is not observed. <b>02/23/10 JG KA</b> Verified the Hardening Procedures EMS PC Unity v.3.2.1.0 2/18/10 clearly states how to recover from the blue screen when an event log becomes corrupt. However, further testing is required on the hardening procedures for stand-alone PC and 2003 Server.	
120	02/12/10	K. Austin	Document Defect	Closed	Voting System Overview Unity v. 3.2.1.0 Rev 6.0 12/30/09 Fig.1.4.1	In Figure 1.4.1 Standalone System - Single EMS Workstation diagram the following issues were identified: a) The Election Coding Center - Results Consolidation and Reporting and Election Coding Center -Equipment	v.2:2.2.1 b The system description shall include written descriptions, drawings and diagrams that present: a description of the operational	MDN - 2.26.2010 - Updated diagram in Section 1.4.1 in the following manner: a) Altered the heading of the coding center a) Newly labeled	Accept 03/01/10 KA Verified in Voting System Overview Unity v. 3.2.1.0 Rev 8.0 02/26/10 1.4.2 a) Newly labeled	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>Preparation areas do not reflect the configuration of the stand-alone PC. These portions of the diagram only list the applications applicable to the functionality and not the stand-alone configuration. This would only be appropriate if the diagram clearly identifies the distinction between the areas of the a diagram that identify functionality and areas that identify the system configuration</p> <p>b) The Election Coding Center - Results Consolidation and Reporting area contains 2 workstations and a printer networked through a hub. It does not show a standalone system with a printer directly attached.</p> <p>c) In a functional diagram of the Election Coding Center - Equipment Preparation, the Hardened EMS client is missing AIMS, which is required to support the burning of the flash memory for the AutoMARK VAT.</p>	<p>environment of the system that provides an overview of the hardware, software and communications structure</p>	<p>environment to reflect system configurations. Altered the description of the EMS system within the Equipment Programming and Results Collection environments to list only applications used and reference back to the coding center configuration for the full list of EMS applications. Revisions for future system releases will use two diagrams; one for network/PC configuration and one for functional environments.</p> <p>b) Updated the Results consolidation environment to reflect real world use in a standalone environment. Printer connected directly to standalone system without hub. Separate instance of ERM runs on a separate PC for report display. Results transferred manually from the standalone EMS PC to the display PC.</p> <p>c) Added AIMS to the equipment preparation environment.</p>	<p>Functional Environment - Election Central: Results Consolidation and Reporting and Functional Environment - Equipment Preparation reflect the a stand alone PC. Reference is made back to coding center configuration for full list of EMS applications.</p> <p>b) Newly labeled Functional Environment - Election Central: Results Consolidation and Reporting displays a stand alone system with an attached printer</p> <p>c) Newly labeled Functional Environment - Equipment Preparation now lists AIMS.</p>
121	02/12/10	K. Austin	Document Defect	Closed	Voting System Overview Unity v. 3.2.1.0 Rev 6.0 12/30/09 Fig.1.4.2	In Figure 1.4.2 Shared EMS File Server - Peer to Peer File Sharing with Windows XP, the following issues were identified: a) In the Election Coding Center - Closed Workshop area , the Hardened EMS Client (Equipment Burning ) workstation appears to be displaying the functionality and configuration of the Results Display workstation (see	v.2.2.2.1 c & f1 The system description shall include written descriptions, drawings and diagrams that present: c. A theory of operation that explains each system function, and how the function is achieved in the	<b>MDN - 2.26.2010 -</b> Updated diagram in Section 1.4.2 in the following manner: a) Updated the Equipment Preparation PC to reflect use of HPM and AIMS rather than ERM.	Accept 03/01/10 KA Verified in Voting System Overview Unity v. 3.2.1.0 Rev 8.0 02/26/10 1.4.2 a) The Hardened EMS Client displays HPM and AIMS and does not display ERM. This

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>Results Consolidation and Report) and not the Equipment Burning functionality.</p> <p>b) In the Election Coding Center - Equipment Preparation area, the Hardened EMS client is missing AIMS, which is required to support the burning of the flash memory for the AutoMARK VAT.</p> <p>c) In the Election Coding Center - Closed Workshop, Election Coding Center Results Consolidation and Reporting, and the Election Coding Center - Equipment Preparation the "Hardened EMS Clients" identify the database location as "c:\elecdata" and not mapped to the shared location on the file server. (The client identified as complete does not identify the database location.)</p> <p>d) In the Election Coding Center - Closed Workshop area there is no description, in text or diagram, that identifies that multiple clients are allowed to access the same election.</p>	<p>design; ...</p> <p>f. Interfaces among internal components, and interfaces with external systems. For components that interface with other components for which multiple products may be used, the TDP shall provide an identification of:</p> <p>1) File specifications, data objects, or other means used for information exchange;</p>	<p>b) Added AIMS to the application listing under the equipment preparation environment</p> <p>c) Updated the diagram to map client PCs more explicitly to the peer to peer server (see text beneath database location for all client icons)</p> <p>d) Added verbiage under the server icon to indicate that multi-user access is allowed.</p>	<p>is consistent with Equipment Burning Functionality</p> <p>b) The Hardened EMS client includes AIMS.</p> <p>c) The diagram now identifies the database location as Q:\Share on the file server.</p> <p>d) The file server now identifies that multiple clients are allowed.</p>
122	02/12/10	K. Austin	Document Defect	Closed	Voting System Overview Unity v. 3.2.1.0 Rev 6.0 12/30/09 1.4.3	<p>In Figure 1.4.3 Locally Networked EMS - Windows 2003 Server, the following issues were identified:</p> <p>a) In the Election Coding Center - Closed Workshop area , the Hardened EMS Client (Equipment Burning ) workstation appears to be displaying the functionality and configuration of the Results Display workstation (see Results Consolidation and Report) and not the Equipment Burning functionality.</p> <p>b) In the Election Coding Center - Equipment Preparation area, the Hardened EMS client is missing AIMS, which is required to support the burning of the flash memory for the AutoMARK VAT.</p> <p>c) In the Election Coding Center - Closed Workshop, Election Coding Center Results Consolidation and Reporting, and the Election Coding Center - Equipment Preparation the "Hardened EMS Clients" identify the</p>	<p>v.2:2.2.1 c &amp; f1 The system description shall include written descriptions, drawings and diagrams that present:</p> <p>c. A theory of operation that explains each system function, and how the function is achieved in the design; ...</p> <p>f. Interfaces among internal components, and interfaces with external systems. For components that interface with other components for which multiple products may be used, the TDP shall provide an identification of:</p> <p>1) File specifications, data objects, or other means used for information</p>	<p>MDN - 2.26.2010 - Updated diagram in Section 1.4.2 in the following manner:</p> <p>a) Updated the Equipment Preparation PC to reflect use of HPM and AIMS rather than ERM.</p> <p>b) Added AIMS to the application listing under the equipment preparation environment.</p> <p>c) Updated the diagram to map client PCs more explicitly to the peer to peer server (see text beneath database location for all client icons)</p> <p>d) Added verbiage under the server icon to</p>	<p>Accept 03/01/10 KA</p> <p>Verified in Voting System Overview Unity v. 3.2.1.0 Rev 8.0 02/26/10 1.4.3</p> <p>a) The Hardened EMS Client displays HPM and AIMS and does not display ERM. This is consistent with Equipment Burning Functionality</p> <p>b) The Hardened EMS client includes AIMS.</p> <p>c) The diagram now identifies the database location as Q:\Share on the file server.</p> <p>d) The file server now identifies that multiple clients are allowed.</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
						database location as "c:\elecdata" and not mapped to the shared location on the file server. (The client identified as complete identifies the database location as "c:\elecdata" but does reference mapping to the D:\ Share on the server.) d) In the Election Coding Center - Closed Workshop area there is no description, in text or diagram, that identifies that multiple clients are allowed to access the same election.	exchange;	indicate that multi-user access is allowed.		
123	02/12/10	J. Garcia	Functional Defect	Closed	Mapping of the shared drive Server-share.exe (script)	The client cannot map to the Q:\elecdata folder on the server.  When executing the "Servershare.exe" script it creates a folder "SymLink" with a link to the "electdata" folder however; the executable did not share the SymLink folder. This prevents the client from mapping to the Q:\elecdata folder.	v. 1.2.2.1.b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.	DWH - 3.8.2010 - Correct the problem in the ServerShare.exe (script)	Accept 03/18/10 JG Executed the new Servershare.exe script per the Hardening procedures and verified that it correctly sets up the SymLink with the electdata folder.	
124	02/22/10	C Coggins	Informational	Closed	1) System Security Spec Ver. Rel. 3.2.1.0 2/17/10  2) M100 SOP FW V. 5.4.3.0, HW Rev 1.3 2/12/10  3) Unity 3.2.1.0 Sys Change Notes Rev 4	Configuration Management: Revised documents were submitted without correctly updating the dates and history.  1) The 2/17/10 date of the Security Spec was not updated on the title pg but it was correctly noted in the footer. Recent updates were not noted in the Ch. 11 Revision History. The order of the history is inconsistent. 2) The M100 SOP date had not been changed on the title pg or footer from the prior release. This update was not noted in the Ch 14 Revision History 3) Unity 3.2.1.0 System Change Notes, the title pg displays revision 3.0 and the pg footers display 4.0.		MDN - 2.26.2010 - Updated dates and revision histories for all listed documents.	Accept 03/01/10 KA 1) Verified in Sys Sec Spec Ver. Rel. 3.2.1.0 2/24/10 the dates on the footer & title page match & the update was reflected in Ch. 11 Revision History; revision history order was consistent. 2) Verified in M100 SOP FW v.5.4.4.0, HW Rev1.3 2/26/10 the title page & footer date are changed; changes are listed in CH 14 Revision History. 3) Verified in Unity 3.2.1.0 Sys Change Notes Rev 4 that the title page & footer display rev 4.0	
125	2/16/10	K. Wilson	Document Defect	Closed	Hardening Procedures EMS PC Unity 3.2.1.0 February	The origin of an ES&S provided executable file cannot be validated  The self-extracting script,	v. 1:8.6.c. Perform the initial delivery and installation of the system to a customer, including	DWH - 3.8.2010 - • In the Hardening Procedures modified Section 1.2 - Added	Accept 03/15/10 KA & KW Verified the Hardening Procedures EMS PC	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
					3, 2010	ServerShare.exe, contains an executable, linkd.exe. This file is not declared in the Hardening document. iBeta was unable to validate the origin of this file.	confirmation that the installed version of the system matches exactly the qualified system version; v.1:4.1.1 Software furnished by an external provider (for example, providers of COTS operating systems and web browsers) where the software may be used in any way during voting system operation; ... v.2:2.2.1.e Identification of all COTS hardware and software products and communications services used in the development and/or operation of the voting system, identifying the name, vendor and version used for each such component	source for Linkd.exe	Unity 3.2.1.0 3/10/10 v.2.4 declares the source for the Linkd.exe. The hash was compared and verified identical to the Linkd.exe downloaded from the Internet.
126	2/19/10	K. Wilson	Docu-ment Defect	Closed	Hardening Procedures EMS PC Unity 3.2.1.0 February 3, 2010 - Shared files in ERM	Access to data in locked files in an application not using RM/COBOL file system is not addressed.  Shared files in ERM: In the RM/Cobol User's Guide First Edition, appendix B it states that "an application not using the RM/COBOL file system can still access data in locked files." This possibility is not addressed in the Hardening Procedure or cross referenced to another TDP document.	v.1:2.2.1.a Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability v.2:2.5.8 The vendor shall identify and provide a diagram and narrative description of the system's databases, and any external files used for data input or output. The information provided shall include for each database or external file: ...e. Details of ... their specifications, including: ... 7) Priority, timing, frequency, volume, sequencing, and other constraints, such as	MDN 03/09/10- Updated ERM SDS provided on 03.09.2010. TDP Rev8a4  GLW 03/08/10: Updated the ERM SDS, Section 3.3, File Sharing, to indicate that there is no file sharing between the ERM RM/Cobol application and other applications. Therefore, there is no file locking issues.	Accept 03/11/10 KW &KA  Verified Section 3.3 of the ES&S SDS ERM Unity v.3.2.1.0 3/8/10 v. 5.0 says "There is no file sharing between RM/COBOL applications and other applications." This addresses access to data in locked files.

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							whether the data element may be updated and whether business rules apply; v.1:7.7.a To meet documentation requirements, vendors shall provide complete product documentation with each voting systems or components, as described Volume II, Section 2 for the TDP. This documentation shall: a. Be sufficient to serve the needs of the ITA ...		
127	2/19/10	K. Wilson	Document Defect	Closed	Hardening Procedures EMS PC Unity 3.2.1.0 2/8/10  Voting System Overview Unity v. 3.2.1.0 2/11/0  Shared files in ERM	Hardening procedure does not provide a warning about using the fully specified file name with Linkd command in Windows.  In reference to shared files in ERM, the RM/Cobol User's Guide First Edition, appendix B states that file locking is accomplished in Windows using the fully specified filename, and warns about the use of the In statement in Unix systems. The linkd command in Windows accomplishes the same purpose as the In command in Unix. The linkd command is used during system hardening. The documentation doesn't address the possibility that files are accessed by ERM locally with a differently qualified name than the same file accessed remotely. The System Overview in Figure 1.4.2 shows that ERM may be installed on the peer-to-peer File Server, and it was installed there during the hardening procedure.	v.1: 2.2.1.a Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability v.2:2.5.8 The vendor shall identify and provide a diagram and narrative description of the system's databases, and any external files used for data input or output. The information provided shall include for each database or external file: ...e. Details of ... their specifications, including: ... 7) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply; v.1: 7.7.a To meet documentation requirements, vendors shall provide complete	DWH - 3.8.2010 - • We discussed this issue with MicroFocus and their reply was: Record locking is handled by RM/Cobol., and file locking is handled by the operating system. They said if the file is locked it is locked, no matter how you get to the file whether from c:\elecdata or q:\elecdata. Re-testing by ES&S, also, indicates locking depends on the file name and not the path.	Accept 4/7/10 JG KA Hardened the PCs using "Hardening Procedures EMS PC Unity 3.2.1.0, 3/10/10, Rev 2.4" and verified that users cannot access the same record. (i.e. Multiple user can update election results for different precincts but can't simultaneously update the election results for the same precinct.)

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							<i>product documentation with each voting systems or components, as described Volume II, Section 2 for the TDP. This documentation shall: Be sufficient to serve the needs of the ITA ...</i>		
128	02/23/10	J. Garcia	Document Defect	Closed	ES&S HPM SOP Ver. Rel.7.2.0 2/12/10 ES&S ERM SOP Ver. Rel. 7.5.6.0 2/12/10 Installation of application	<p><i>The HPM and ERM SOPs do not reference a key element in setting up a networked EMS PCs.</i></p> <p><i>The HPM SOP (Ch 3: installation) and ERM SOP (Ch 5: Install Election Reporting Manager) do not reference the section on Change Control File. When setting up either the P2P or Client Server configurations a user must go to the Change Control File and set up the network drive, however, this is not stated in either document until Ch 34 of the HPM SOP and Ch 42 of the ERM SOP and long after installation has occurred causing an incorrect flow of the system functions.</i></p>	v.2: 2.8.5.b. Provides procedures that clearly enable the operator to assess the correct flow of system functions	<p><b>DJZ - 2-26-10</b> - User should follow steps outlined in ES&amp;S ERM SOP, Ch 2: Pre-Election Tasks. Reference to verify Control File settings is step #4 on pg 12.</p> <p><b>HPM SOP</b> - In Ch 2: Hardware Programming Procedures under the Install HPM heading, the user is informed that if this is the first time to install the software they must go to Ch 3: Installation. When the user goes to Installation chapter and if they follow the instructions set forth in the SOP the note to check the Control File is at the end of these instructions.</p>	<b>Accept 03/08/10 - KA &amp; JG - Verified in HPM SOP Ver. Rel. 5.7.2.0 2/22/10 (Ch 3: installation) and ERM SOP Ver. Rel. 7.5.6.0 02/22/10 (Ch 5: Install Election Reporting Manager) now reference the section on Change Control File.</b>
129	2/26/10	K. Austin	Document Defect	Closed	Hardening Procedures For EMS PC Unity v.3.2.1.0 2/18/10 v.2.2	<p><i>The Hardening Procedures do not have a warning concerning the consequences of deleting the Symlink NTFS junction point folder.</i></p> <p><i>Deleting an NTFS junction point will cause the contents of its target folder to also be deleted. It is expected that system administrators can delete files. The concern is that the system administrator may not fully understand the consequences of deleting the SymLink folder. The procedure has no warning to advise an administrator that the target folder can disappear if for some reason during the hardening</i></p>	v.2:2.4.2 The vendor shall provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for qualification testing.	<b>DWH 03.09.10</b> - Modified the Hardening Procedures - Appendix K - added warning statement addressing this issue.	<b>Accept 03/11/10 KA – Verified the Hardening Procedures EMS PC Unity 3.2.1.0 3/10/10 v.2.4 contains a warning addressing the deletion of the SymLink folder.</b>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						process the folder is deleted and scripts are rerun. The loss of the target occurs not when the folder is deleted but when the trash is emptied. This can make it difficult for the administrator to connect the problem back to the deletion of the SymLink folder. This is not a concern for any other user, as the system hardening prevents access to and deletion of these folders.			
130	3/5/10	J. Garcia	Docu- ment Defect	Closed	Unity 3.2.1.0 System Change Notes rev04 (no date)	The submitted M100 change notes do not identify the changes between the different version release. It is unclear if the list provided is comprehensive.	v.2.2.13b A listing of the specific changes made, citing the specific system configuration items changed and providing detailed references to the sections of documentation changed	<b>MDN 03.12.10</b> - Added item 17329 to the Model 100 section of the change notes document. The system change notes document all changes to the system that occurred between introduction of the Model 100 to the Unity 3.2.1.0 system and the current date.	<b>Accept 04/02/10 KA</b> Verified the Unity 3.2.1.0 System Change Notes Rev 7.0 (no date) includes changes and item 17329 for the Model 100.
131	3/5/10	J. Garcia	Docu- ment Defect	Closed	Unity 3.2.1.0 System Change Notes rev04 (no date)	System Change Notes document don't identify enhancements or bug fixes.  The System changes notes do not reflect all of the submitted DS200 changes BUG16775, ENH14725 ENH14726, ENH14728, ENH14729, ENH14730, ENH14731, ENH14732, ENH14745, ENH15009, ENH15287, ENH15288, ENH15418, ENH15890, ENH15891, ENH15892, ENH16085, ENH16120, ENH16211, ENH16291, ENH16336, ENH16382	v.2.2.13b A listing of the specific changes made, citing the specific system configuration items changed and providing detailed references to the sections of documentation changed	<b>MDN 03.11.10</b> - All listed items are included in revised system change notes provided with TDP Rev8a4 - 03092010.	<b>Accept 03/23/10 SE</b> Verified in System Change Notes Rev06 now references all of the listed bugs and enhancements.
132	3/8/10	S.Eaton	Funcitio- nal Defect	Closed	Unity HPM v. 5.7.2.0	Enhancement notes are inconsistent with HPM functionality and documentation.  ES&S provide responses to questions regarding changes to the DS200. In the DS200 - 1 4 1 0 Questions ERW ENH14745 spreadsheet, ES&S states "Five new buttons have been added to allow poll workers to override the election query settings for blank ballots, overvotes, cross-overs, marginal (unreadable?) marks, and undervotes." There is no undervote query	v.2.2.6c Election Management System The Election Management System (EMS) is used to prepare ballots and programs for use in casting and counting votes, and to consolidate, report, and display election results. An EMS shall generate and maintain a database, or	<b>JML 03.23.10</b> - Undervote functionality is defined in EDM not HPM. EDM SOP describes setup of Query Undervote in Ch 25 pg 224 for Contests and Ch 39 pg 299 for Text/Referendum. Undervote Queries must be set up by individual contests/referendums. If the Query Undervote	<b>Accept 03/25/10 SE</b> Verified EDM SOP Ch 25 and 39 inform the tester of the Query Undervote option, and was also verified during testing.  <b>Reject 03/23/10 SE</b>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>enhancement/feature found in the HPM application or user documentation</p> <p><b>03/23/10 SE Rejected:</b> In HPM all available fields have been set to Query. (Blank, Overvote, Cross-over and Marginal.) There is no Undervote query field in HPM. With these settings, the blank, overvotes, cross-overs, and marginal buttons are active. The button to override the undervote query is grayed out and inactive. There are no options available to make this button active.</p>	<p>databases, that enables election officials or their designees to perform the following functions: c. Define ballot formats and appropriate voting options</p>	<p>flag is set for any contest or Text/Referendum, then the Undervote Query Override option becomes available on the DS200 Polls Opened Menu.</p> <p><b>SLM 03.11.10 -</b> Enhancement 14745 will only be visible on the DS200. There is nothing special in HPM that needs to be set for this enhancement. If the DS200 is set for query in HPM, you will be able to select these new query options on the DS200. That is why there is no information about this enhancement in the HPM SOP.</p>	
133	3/8/10	J. Garcia	Docu- ment Defect	Closed	AIMS Election Officials Guide Rev 19, 2/16/10	<p>References to networking in the AIMS and Hardening procedures are inconsistent</p> <p>In section 2.2 System (Administrator Responsibilities) it states "The AIMS computer should not be networked with other computers. The AIMS computer should not be used for any other purpose other than running AIMS and Microsoft Excel." This is inconsistent with networking in the hardening procedures.</p>	v.2: 2.3  <p>The vendor shall provide a listing of the system's functional processing capabilities, encompassing capabilities required by the Standards and any additional capabilities provided by the system such as maximum # of contest per a single ballot style</p>	<p><b>MDN 03.11.10 -</b> Updated Section 2.2. of the AIMS Election Officials Guide to require system administrators to set up the AIMS PC according to the policies and procedures included in the ES&amp;S Hardening the Election Management System PC document.</p>	<p><b>Accept 03/23/10 SE -</b> Verified in AIMS Election Officials Guide rev.20 now states that the System Administrator should set up the AIMS computer according to the procedures and policies outlined in the ES&amp;S Hardening Procedures document.</p>
134	3/9/10	K. Wilson	Docu- ment Defect	Closed	Jurisdiction Security Procedures ES&S v.1.0.0.1 5/8/08	The JSP Template contains multiple places where telecommunications is addressed and allowed. As a template, this is acceptable, but the template does not address making the determination as to whether telecommunications is allowed at all based on the EAC certification of the system being used. The document contains the following references to telecommunications (as defined by the EAC). While this template may be an overall document covering all	v.1: 7.5.4 Ballot recording and vote counting can be performed in either a dedicated or non-dedicated environment. If ballot recording and vote counting operations are performed in an environment that is shared with other data processing functions, both hardware and software features	<p><b>MDN 04.16.2010 --</b> Submitted with TDP Rev9a2 2010.04.16.</p> <p><b>BB 03.11.20 --</b> Added two warning messages to the manuals. One warning was for Network Admins to review V:1, S:7.5 and 7.6 prior to configuring a voting system network.</p>	<p><b>Accept 4/29/10 JG</b> Verified the Jurisdiction Security Procedures ES&amp;S v.1.0.0.1 5/8/08 has a warning for telecommunication usage. See discrepancy 158 for the JSP document versioning and date not changing.</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>networks associated with a jurisdiction, it does not address isolating a voting network from other jurisdictional networks. The following sections of the document imply connections of a network to a telecommunications system.</p> <p>1.2.3 -- VPN, DMZ and FTP          1.2.4 -- FTP, DMZ          2.1.3.1.1 -- telephone, FAX, Internet          2.1.3.1.5 -- On-line data          2.1.3.1.6 -- On-line ordering          2.1.3.1.8 thru 2.1.3.1.10 -- email, web browsers, Internet and Subscription Services          2.1.3.1.14 -- telephone and web conferencing          5.9 -- Electronic Commerce Services (entire section &amp; subsections)          5.10.6 -- Clock Synchronization          6.7 -- Mobile computing and telecommuting (entire section &amp; subsections)</p> <p><b>Rejected JG 04/09/10 - No updated document received.</b></p>	<p>shall be present to protect the integrity of vote counting and of vote data. Systems that use a shared operating environment shall:</p> <ul style="list-style-type: none"> <li>a. Use security procedures and logging records to control access to system functions</li> <li>b. Partition or compartmentalize voting system functions from other concurrent functions at least logically, and preferably physically as well</li> <li>c. Control system access by means of passwords, and restrict account access to necessary functions only</li> <li>d. Have capabilities in place to control the flow of information, precluding data leakage through shared system resources</li> </ul>	<p>The second warning message was for users to be cognizant of the laws and restrictions that apply when implementing a voting system and used telecommunications usage as an example.</p>	<p><b>Reject JG 04/09/10</b></p>
135	3/13/10	K. Austin	Docu- ment Defect	Closed	<p>Hardening Procedures EMS PC Unity v.3.2.1.0 2/18/10 v.2.2</p> <p>Voting Sys Overview Unity v.3.2.1.0 v.8.0 02/26/10.</p>	<p>The Hardening Procedures and the System Overview do not identify that only Windows 2003 Server R2 32 bit Operating System is compatible with the rest of the hardening process.</p> <p><b>Rejected SE 03/25/10 - No updated document received.</b></p>	<p>v.2.2.4.2 The vendor shall provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for qualification testing.</p>	<p><b>MDN 04.06.10 -</b> Updated all sections of the System Overview that reference a Windows Operating System to explicitly restrict the OS to 32-bit installations. Revised overview provided with TDP Revision 9 (4.9.2010).  <b>MDN 03.22.10 -</b> Updated Section 1.2.2. of ES&amp;S Voting System Overview to specify that only the e32-bit version of Windows 2003 server is supported by the ES&amp;S voting system..</p>	<p><b>Accept 4/12/10 KA</b>          Verified Voting Sys Overview Unity v.3.2.1.0 v.10.0 04/06/10 clearly identifies and restricts the OS to 32-bit . The Hardening Procedures EMS PC Unity v.3.2.1.0 3/10/10 v.2.4 references the Overview as a required document.</p> <p><b>Reject SE 03/25/10</b></p>
136	03/20/10	J. Garcia	Func- tional	Closed	EMS LAN PCs Mapping to Q &	HPM/ERM Manager Security settings do not restrict access on EMS LAN PCs	v.2.2.2.5.3 Third, the system shall be configured	<b>SLM 03.23.10 -</b> HPM/ERM Manager is	<p><b>Accept JG 4/12/10</b>          Replacement of HPM</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
			Defect		ERM 7.5.6.0 HPM 5.7.2.0 Security Procedures settings	<p>mapped to the Q drive.</p> <p>ERM/HPM have security settings to restrict user groups to specific functionality. After hardening each of the networked PCs and adding multiple users within the ElectDefine and ElectResult groups the security settings in ERM/HPM Manager are set up. To set up: create and add digit IDs, update and exit ERM/HPM Manager. Log in as one of the new ElectResult users and double click on ERM. At this point the user should see "Enter your User ID" however the application does not display this window and allows the user to continue into ERM without entering the User ID. All users have complete access to all application functionality. This also occurs with the HPM user.</p> <p><b>Rejected CEC 3/24/10 - Discrepancy #103 was closed by restricting users in HPM/ ERM Manager . If this functionality is withdrawn #103 will be reopened.</b></p>	<p>to execute only intended and necessary processes during the execution of election software.</p> <p>v.1:2.2.1.a Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability</p>	<p>not supported or associated with Unity 3.2.1.0. ES&amp;S replaced the HPM/ERM Manager in Unity 3.2.0.0 with the hardening procedures.</p> <p>HPM SOP - Removed Ch 5</p> <p>ERM SOP - Removed Ch 7</p>	<p>&amp; ERM Manager access controls with the Windows controls is being reviewed for requirements met by the withdrawn functionality. As a result, discrepancy #103 is reopened.</p> <p>Verified HPM SOP - Ver. Rel. 5.7.2.0 4/8/10 Removed Ch 5 and ERM SOP Ver. Rel. 7.5.6.0 4/8/10 Removed Ch 7.</p> <p><b>Reject CEC 3/24/10 -</b></p>
137	03/20/10	C Coggins	Functional Defect	Closed	VAT - Summary Screen Audio, Repeating Instructions	<p>Summary Screen navigation and functional audio instructions cannot be repeated after the voter starts reviewing contests and selections.</p> <p>Upon entering the Summary Screen audio instructions regarding reviewing the selections and changing votes are played. Prior to moving into the review of a contest the voter can repeat these instructions. Once they've moved into the summary list the instructions cannot be repeated. Exiting and reentering the Summary Screen does not permit access to these instructions.</p>	v.1: 2.2.7.2.b.5 Provide audio information and stimulus that: Enables the voter to request repetition of any information provided by the system.	<p><b>HD 03.25.10 - The AutoMARK is working as designed. The design is such that you can go into the summary and use the previous button to return to the contest listing and then use the next button to return to the summary, it will always repeat the instructions. Once you select a contest for modification and return to the summary screen, exiting and returning to the summary will play back that contest to confirm the modification that the voter made</b></p>	<p><b>Accept 4/2/10 CEC</b> ES&amp;S' response is being accepted because the flow they describe is how the machine is likely to be used. It represents a logical and clear path for an audio ballot user. Navigation instructions can be repeated at the time they are played. The design serves the more linear nature of the audio ballot.</p> <p><b>Accept 5/18/10 JG</b> The voter has the option to return their ballot at any time and start over. Verified v.1: 2.2.7.b.3 voter has the same vote</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
									capabilities and options as those provided by the system to individuals who are not using audio technology.
138	03/21/10	C Coggins	Func-tional Defect	Closed	VAT - Pick-a-party Open Primary	<p>On an audio ballot, one contest in a pick-a-party open primary ballot can be marked for two parties . The visually displayed ballot does not follow the audio,</p> <p>This issue is observed in a very narrow set of parameters and by following a very specific sequence of steps. The election must be a Pick-a-Party Primary. Party selection cannot be the last party in the list. A non-partisan contest must be on the ballot after the partisan primary contests. The voter must be listening to the audio ballot and return to the non-partisan contest from the Summary Screen. The voter must select the back button on the non-partisan contest. At this time the screen remains on the non-partisan contest and the audio plays a candidate name of the last partisan primary contest of the last party on the ballot. It appears that the candidate name that is played is dependent upon the "Vote for" and the number of selections made when the primary contest was voted. (Example: DEM party is picked; the DEM contest is a "Vote for 2" with 2 candidates selected. The audio plays the corresponding REP contest with REP candidates selected. These REP selections are affected by the position of the DEM candidate selections.) The voter can now make changes. However regardless of the selection it changes only the first two candidates in the list. Visually these selections are displayed on the Y/N non-partisan contest. At times selections for both Yes and No were marked. (Testing confirmed the behavior wasn't observed if party selection differed from above. The</p>	v. 1: 2.4.2.c To activate the ballot, all DRE systems shall: Prevent a voter from voting on a ballot to which he or she is not entitled (This requirement is applicable because the VAT performs the ballot display functions of a DRE.)	<b>SLM 04.06.10</b> - This issue is addressed with AutoMARK version 1.3.2907.	<b>Accept 04/27/10 DVJG</b> Verified in v. 1.3.2907 that the audio and visual ballots remained in sync and the contests for the non-selected party could not be accessed.

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						test election contained these specific variables: 2 parties only; non-partisan contest was a question and not a race; and the contest before the non-partisan contest was a vote for 2. )			
139	3/24/10	S Eaton	Document Defect	Closed	Unity 3.2.1.0 System Change Notes v7.0	The System Change Notes document does not address BUG16384.	v.2:2.13b A listing of the specific changes made, citing the specific system configuration items changed and providing detailed references to the sections of documentation changed	<b>MDN 04.06.10 - BUG16384 is associated with Election Reporting Manager software in ES&amp;S' defect tracking system. The listing for BUG 16384 appears in Section 2.2. of the Unity 3.2.1.0 System Change Notes rev. 7.0. Document rev7.0 delivered with TDP_Rev8a6_20100312</b>	<b>Accept 4/12/10 KA</b> Verified Unity 3.2.1.0 System Change Notes v8.0 addresses BUG16384.
140	3/25/10	J. Garcia	Functional Defect	Closed	ERM v.7.5.6.0 Collect ballot images	DS200 ballot images uploaded through ERM can not be viewed.  DS200 Ballot images (voted paper ballots) are stored in c or Q :\elecdatal\election name\DS200\ images. The images are saved as Raw Images however the images can not be viewed. There is no functionality within the ERM to view the images. There is no application or image viewer identified within the hardened system configuration.	v.1:2.2.1.b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions. v.2: 2.8.5a The vendor shall provide documentation of system optioning procedures: Provide a detailed description of procedures required to initiate, control, and verify proper system operation.	<b>DMZ 05.03.10 ERM SOP-</b> Added Note ERM does not provide functionality for viewing collected ballot images. The ballot images can be copied from the hardened system for viewing on a PC platform independent from the Unity Election Management System with various third-party applications	<b>Accept 5/4/10 KA</b> Verified the ERM SOP Ver. Rel. 7.5.6.0 5/3/10 states that ballot image bitmaps must be transferred to a PC out of the EMS network and viewed with a 3rd party application.
141	3/25/10	J. Garcia	Document Defect	Closed	HPM SOP v.5.7.2.0 and ERM SOP v.7.5.6.0 2/22/10	The HPM and ERM SOP do not address the LAN configurations.  Both SOPs do not provide instructions for the Peer-to-Peer and Windows 2003 Server-share.exe script 3 EMS configurations. All references are to the C drive. There is no reference to the networked Q drive.	v.2: 2.8.5a  The vendor shall provide documentation of system optioning procedures: a. Provide a detailed description of procedures required to initiate, control, and verify proper system operation.	<b>4-7-10 DJZ -</b> Added note to reference (Refer to Hardening Procedures for the Election Management System PC for information on setting up Peer-to-Peer and Windows 2003 EMS configurations) in the Installation chapter. Also added throughout the SOP - This folder is	<b>Accept 4/12/10 KA</b> Verified in HPM SOP v.5.7.2.0 and ERM SOP v.7.5.6.0 4/8/10 that the LAN configuration is addressed by referencing the mapped network drive (Q drive).

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								located on the local disk (C:) or the mapped network drive.), where needed to reference the C: drive and network drives.	
142	3/25/10	J. Garcia	Document Defect	Closed	ES&S HPM SOP Ver. Rel. 5.7.2.0 2/22/10 Ch 13: Jurisdiction	HPM SOP does not address changes to System Type.  On pg 69 of Ch. 13 it states, "From the System Type list, select Both. This is the only equipment type being supported by ES&S. <b>NOTE:</b> The Central Count, Precinct Count, and Mixed system types are not supported." Discrepancy #20 contradicts this statement. A fix was submitted in ERM v.7.5.5.0 to address various equipment types.	v.2: 2.8.5.a The vendor shall provide documentation of system operating procedures that meets the following requirements: a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation	<b>4-7-10 DJZ</b> - Added information about System Types in Ch 12: Jurisdiction.	<b>Accept 4/14/10 KA JG</b> – Verified HPM SOP Ver. Rel. 5.7.2.0 4/8/10 addresses changes in the system type and the 4 system types (central count, precinct count, both and mixed mode) are supported.
143	3/29/10	K. Austin	Functional Defect	Closed	ES&S DS200 v.1.4.3.0	The DS200 accepted counterfeit ballots produced by copying a valid ballot on blank ballot stock.  The DS200 accepted counterfeit ballots produced by copying a valid ballot on blank ballot stock. ES&S provided the ballot stock. ES&S confirmed the scanner detection is the ink and not any special marks printed on the ballot. The valid ballot was also copied onto regular copier paper. The DS200 was calibrated following the DS200 SOP 2/12/10 procedures for the counterfeit ballot calibration. A successful calibration message was displayed. These ballots were read by the scanner. They were not detected as counterfeit.	v.1: 2.2.1.b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.	<b>MDN 04.09.10</b> - ES&S has withdrawn support for DS200 counterfeit ballot detection from Unity 3210. Added a note indicating non-support of this functionality to the DS200 SOP, Ch 5, "Pre-Election Day Tasks: Calibrate Counterfeit Ballot Sensor"	<b>Accept 4/12/10 KA</b> Verified in ES&S DS200 System Ops Procedures HW v. 1.2.1 FW v. 1.4.3.0 4/8/10 states "Note: The current Unity release does not support counterfeit ballot detection"
144	4/1/10	J. Garcia	Functional Defect	Closed	ERM v.7.5.6.0 Number Key-District Only report	Report displays ballots cast equipment totals incorrectly after add/change groups.  After creating a database for 4 groups, results from the first 2 of the 4 groups were read. The Group Description in the Add/Change Groups option was updated. The first group read in was moved to the bottom of the list and everything else moved up one position. The user ran the Number Key - District Only report. The	v.1: 2.5.3.1g All systems shall provide capabilities to: Prevent data from being altered or destroyed by report generation ...  v.1: 4.4.4a At a minimum vote tally data shall include: Number of ballots cast ... by tabulator.	<b>MDN 06.07.10</b> -- Issue corrected with ERM version 7.5.7.0. <b>GLW 04.06.10</b> - The Add/Change Groups maintenance screen does not alter the contents (tabulated results) of the ERM group into which results have been processed. Additionally, no ERM	<b>Accept 08/04/10 JG &amp; SAB</b> Loaded ERM 7.5.7.0 rev 06-16-10, then installed REG1S1EN from DS200 Functional test case onto PC. Needed to copy all M100Demo data from C: elecdata to Q:elecdata for ERM to view election on Q

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>groups correctly moved to the updated positions however, the results did not move. The group totals remained in their original positions so that the group totals were incorrectly displayed.</p> <p><b>Rejected 4/15/10 JG:</b> iBeta understands that it may not be a common practice to change Add /Change Groups however; this option is available and allows a user to move and/or added groups. When this happens the results do not move with the description. This makes the total incorrect to the groups. This issue was originally identified by SysTest in Unity 4.0. Issue 9 was brought over from the Unity 4.0 test effort. The tester stated that when they imported the results with 4 or more groups the totals did not match the groups. SysTest used the Add/Change Groups, which did not correct the issue. iBeta closed disc #9 because the results imported correctly. We followed the test scenario outlined by SysTest to confirm the Add/Change Groups functioned correctly. It does not and as such the report displays the totals incorrectly.</p>		<p>results reports alter the tabulated results once the results have been processed into one of the define ERM Groups.</p> <p>During the initial ERM database create process, the user defines the number of groups to be used for the current election, assigns a Group Description to each (ie, type of voting) and indicates the equipment type to be processed into each respective group. This step is synonymous to inserting Column Names into a spreadsheet file. Once data has been loaded or entered into the respective column cells, changing the Column Name has no effect on the contents of the cells in that column.</p> <p>It is not common practice to change the Group Description or equipment selected for a specific group once the user has created the ERM database, having defined the number of and description of each desired ERM Group,. If the ERM user does need to move results that have been processed into ERM from one group to another, the Copy Results from the Miscellaneous Menu is used to select the group</p>	<p>drive. Once copied, able to view REG1S1EN data in ERM. Only 2 of the 4 groups had totals assigned to them.</p> <p>Attempted to change all 4 groups. The 2 groups with totals assigned to them could no longer be changed. Only the unassigned groups could be changed, or a new group added/changed. Changes included renaming the Group Description and changing the Equipment field.</p> <p><b>Reject 4/15/10 JG</b></p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							<i>to be copied and the Merge Results from the Update Menu is used to select the group into which the results from the selected ERM group will be moved to. In this case, the ERM user would normally use the Add/Change Group screen to assign the appropriate Group Description to both the "old" and "new" ERM groups. Even this process does not alter or destroy any tabulated results or data processed into ERM from the voting system tabulators. This process simply moves data from one ERM Group to another ERM Group.</i>		
145	4/5/10	J. Garcia	Informational	Closed	ERM Help Topics (SOP 7.5.4.0)	ERM Help Topics contain an older version of the ERM SOP  The ERM application contains a quick help provided by the ERM SOP document. The current version of ERM SOP is 7.5.6.0 dated February 22, 2010 however, the quick help topics within ERM opens ERM SOP 7.5.4.0 dated June 18, 2009.		<b>MDN 06.07.10</b> -- Help file has been updated with ERM v. 7.5.7.0. <b>MDN 04.07.10</b> – Acknowledged. Quick Help for ERM in Unity 3210 opens a PDF file of the final System Operations Procedures Manual. This book has been updated over the course of certification for Unity 3210. ES&S will explore whether replacing the PDF help file with the updated book affects certification.	<b>Accept 07/20/10 SAB</b> Verified ERM v.7.5.7.0 contains v.7.5.7.0 help file (PDF)
146	4/5/10	J. Garcia	Functional Defect	Closed	HPM 5.7.2.0 Load Memory Device with Parameters	The election data is not properly being installed on the M650 Zip.  If an election is created with a System Type of "Both", "Precinct Count" or "Central Count" HPM writes the .OFC,	v. 1.2.2.6.d. An EMS shall generate and maintain a database ...that enables election officials ... to ....: generate ... election specific programs for vote	<b>4-7-10 - DJZ</b> - Added information regarding the Mixed Mode option, in Ch 23: Load Memory Device With Parameters - Load the Zip Disk with	<b>Accept JG 4/22/10</b> Tested and verified the HPM SOP 5.4.2.0 4/08/10 ch 23 pg 240 states file (AB.OFC, AB.PRE, AB.RPT,

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						.PRE, RPT, & .RPF files to the M650 Zip. If the election is created "by style" with a System Type of "Mixed Mode" AB is added to the file name (AB.OFC, AB.PRE, AB.RPT, AB.PRF) and the files aren't written to the M650 zip disk.	recording and vote counting equipment.	M650 Mixed Mode Parameters.	AB.PRF) have to be manually copied to the zip.
147	4/5/10	J. Garcia	Document Defect	Closed	ES&S HPM SOP Ver. Rel. 5.7.2.0 2/22/10	<p>There is no documentation regarding transferring the AB.OFC, AB.PRE, AB.RPT, AB.PRF files to the M650 Zip.</p> <p>If an election is created "by style" with a System Type of "Mixed Mode" AB is added to the file name (AB.OFC, AB.PRE, AB.RPT, AB.PRF) and these files are not written to the M650 zip disk. There is no information about this function or how to get the files to the zip.</p>	v.2: 2.8.5.a The vendor shall provide documentation of system operating procedures that meets the following requirements: a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation	<b>4-7-10 - DJZ</b> - Added information regarding the Mixed Mode option, in Ch 23: Load Memory Device With Parameters - Load the Zip Disk with M650 Mixed Mode Parameters.	<b>Accept 4/12/10 KA</b> Verified the ES&S HPM SOP Ver. Rel. 5.7.2.0 2/22/10 documents the transferring of the AB.OFC, AB.PRE, AB.RPT, & AB.PRF files to the M650 Zip.
148	4/12/10	J. Garcia	Document Defect	Closed	ES&S SFD ERM Unity v. 3.2.1.0 REV 3.0 1/8/10	<p>Sections within the Functional Design Spec identify the ERM password protection functionality for ERM user's access rights which has been removed from Unity 3.2.1.0.</p> <p>Sections 1.1.1 a, f &amp; g, 1.1.5.2 and 2.1 identify "Security Procedures" pertaining to ERM application password protection and creating multiple ERM users with different access rights. This functionality has been removed per the response in discrepancy #136.</p>	v.2:2.5.4 The vendor shall provide information that can be used by an ITA or state certification board to support software analysis and test design. v.1:2.2.1.g System security is achieved through.... capabilities ... administrative practices. To ensure security, all systems shall: Provide documentation of mandatory administrative procedures for effective system security.	<b>04.16.2010</b> Beth Binger-Dunaway  ERM SFD Updated Sections 1.1.1.a,f, and g (pg 5 and 6), 1.1.5.2 (pg 122), and 2.1 (pg 145).	<b>Accept 4/20/10 KA</b> Verified the ES&S SFD ERM Unity v. 3.2.1.0 Rev 4.0 4/16/10 Sect. 1.1.1.a,f, and g (pg 5 and 6), 1.1.5.2 (pg 122), and 2.1 (pg 145) have been updated and do not refer to multiple ERM users.
149	4/12/10	J. Garcia	Document Defect	Closed	ES&S SSS Ver. Rel. 3.2.1.0 2/24/10	<p>The Security Spec statement regarding password protection of software products is inconsistent with the supported functionality.</p> <p>The section Software Product-Specific Security on pg 20 of the Security Spec states "<b>All</b> of the software products in the Unity Software Suite contain password protection" however, HPM and ERM application are not password protected with the removal of ERM and HPM Manager Security Procedures. See discrepancy 136.</p>	v.2:2.5.4 The vendor shall provide information that can be used by an ITA or state certification board to support software analysis and test design. v.1:2.2.1. g System security is achieved through.... capabilities ... administrative practices. To ensure security, all systems shall: Provide documentation of mandatory administrative procedures for effective	[pmz 20100416] Every user has a unique user identifier and password to the system. So, no user can get to ANY of the EMS without a password. Documentation was updated to clarify password protection on pg 20 of the System Security Specification.	<b>Accept 4/20/10 KA</b> Verified the ES&S SSS Ver. Rel. 3.2.1. 4/16/10 no longer states all of the products are password protected, It says very user has a unique identifier and password.

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
150	4/12/10	J. Garcia	Document Defect	Closed	ES&S OVR Unity Ver. Rel. 3.2.1.0 REV 10.0 4/6/10	<p>The Overview statement regarding password protection of software products is inconsistent with the supported functionality.</p> <p>Pg 20 of the Overview identifies ERM and HPM applications to be password protected creating multiple users with different access rights. This functionality has been removed per the response in discrepancy #136.</p>	<p>v.2:2.5.4</p> <p>The vendor shall provide information that can be used by an ITA or state certification board to support software analysis and test design.</p> <p>v.1:2.2.1 g System security is achieved through.... capabilities ... administrative practices.</p> <p>To ensure security, all systems shall: Provide documentation of mandatory administrative procedures for effective system security.</p>	<p><b>MDN 04.16.10 - Updated Section 2.3.2 to remove indicated support for application managed password controls for ERM and HPM (ERM Manager and HPM Manager).</b></p>	<p><b>Accept 4/20/10 KA</b></p> <p>Verified the ES&amp;S OVR Unity Ver. Rel. 3.2.1.0 REV 11.0 4/16/10 no longer identifies ERM and HPM applications to be password protected creating multiple users with different access rights.</p>
151	4/14/10	A Mayer	Document Defect	Closed	AutoMARK VAT 1.3.2907 Software and Firmware Compilation Instructions, ver. 1, 4/09/10	<p>Build document, section 5.2.1 pg 7. Instructions list script name as "TrustedBuildVAT.au3", actual name is "TrustedBuild.au3".</p>	<p>v.1: 8.5.a :The vendor shall establish such procedures and related conventions, providing a complete description of those procedures used to:</p> <p>a. Develop and maintain internally developed items;</p> <p>EAC Voting System Testing and Certification Program Manual, v.1.0 Sec 5.5.1. Demonstrate that the software was built as described in the Technical Data Package.</p>	<p>AutoMARK VAT 1.3.2907 Software and Firmware Compilation Instructions, ver. 2 4/14/10</p>	<p><b>Accept 4/14/10 AM –</b></p> <p>Verified script name is corrected in doc v.2, 4/14/10.</p>
152	4/14/10	A Mayer	Document Defect	Closed	AutoMARK VAT 1.3.2907 Software and Firmware Compilation Instructions, ver. 1, 4/09/10	<p>Build document, section 6, page 13. All cases where instructions include folder name containing "AutoMARK(i)" should be "AutoMARK" (no "(i)"). Document omits steps to copy files "amcode.exe" and "w32code.dll" from C:\Trusted Build\INSTALL Creator to (staging):\Unity 3.2.1.0\Staging\Output.</p>	<p>v.1: 8.5.a: The vendor shall establish such procedures and related conventions, providing a complete description of those procedures used to:</p> <p>a. Develop and maintain internally developed items;</p> <p>EAC Voting System Testing and Certification Program Manual, v.1.0 Sec 5.5.1. Demonstrate that the software was built</p>	<p>AutoMARK VAT 1.3.2907 Software and Firmware Compilation Instructions, ver. 2 4/14/10</p>	<p><b>Accept 4/14/10 AM –</b></p> <p>Verified steps to copy files are provided in doc v.2, 4/14/10.</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							as described in the Technical Data Package.		
153	4/15/10	J. Garcia	Document Defect	Closed	ES&S SDS ERM Unity v. 3.2.1.0 REV 5.0 3/09/10  ES&S SDS HPM Unity v. 3.2.1.0 REV 3.0 01/08/10	<p>The Software Design Specs statements regarding password protection of software products is inconsistent with the supported functionality.</p> <p>Pg 74, 94 and 117 of the ERM SDS call out the "UERMMngr.COB, LOGIN.COB" &amp; "UERMMngr.PWL". Pg 33, 36, 47, 48, 55, 76, 107 &amp; 286 of the HPM SDS call out the "UHPMMngr.COB, HPM.COB, PR074ALL.COB, LOGIN.COB" and "UHPMMngr.PWL" These items are used to set and store the HPM/ERM application passwords. This functionality has been removed per the response in discrepancy #136.</p>	v.2:2.5.4  The vendor shall provide information that can be used by an ITA or state certification board to support software analysis and test design.  v.1:2.2.1.g System security is achieved through.... capabilities ... administrative practices. To ensure security, all systems shall: . Provide documentation of mandatory administrative procedures for effective system security.	<p><b>04.16.2010</b> Beth Binger-Dunaway <u>ERM SDS</u> Removed UERMMngr.COB, LOGIN.COB, and UERMMngr.PWL from lists in Section 3.5 (pg 21), Section 3.6 (pg 57), Section 3.7 (pg 74), and Section 3.8 (pg 93). Removed reference to ERM Security Program Call Structure (pg 154), Program Compile List (pg 212 and 213), and Section 7.2 Programming Specifications Detail (pg 345). Updated section 6.2.7 Security Monitoring and Control (pg 114). <u>HPM SDS</u> Removed UHPMMngr.COB and LOGIN.COM from lists in Section 3.5 (pg 19), Section 3.6 (pg 35), Section 3.7 (pg 51), and Section 3.8 (pg 58). Removed reference to HPM Security Program Call Structure (pg 150), Program Compile List (pg 190), and Section 7.2 Programming Specifications Detail (pg 301). Updated section 6.2.7 Security Monitoring and Control (pg 112). I did not remove any references to PR074ALL.COB as this program is the Copyright Screen</p>	<p><b>Accept 0429/10 JG</b> Verified the removal of UERMMngr. COB, LOGIN.COB, and UERMMngr. PWL in the ES&amp;S SDS ERM Unity v. 3.2.1.0 REV 6.0 4/16/10</p> <p>Verified the removal of UERMMngr. COB, LOGIN.COB, and UERMMngr. PWL in the ES&amp;S SDS HPM Unity v. 3.2.1.0 REV 4.0 04/16/10</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
154	4/15/10	K. Austin	Document Defect	Closed	ES&S SHS DS200 Unity v.3.2.1.0 REV 3.0 01/04/10	<p>The System Hardware Specs for the DS200 contains statements regarding the counterfeit ballot detection sensor that are inconsistent with the supported functionality.</p> <p>Pg 34 and 35 of the ES&amp;S Sys. HW Spec. Unity v.3.2.1.0 describe the counterfeit ballot detection sensor. However, the functionality for the counterfeit detection has been withdrawn per the response in discrepancy #143</p>	v.2:2.5.4  The vendor shall provide information that can be used by an ITA or state certification board to support software analysis and test design. v.1:2.2.1 g System security is achieved through.... capabilities ... administrative practices. To ensure security, all systems shall:.. Provide documentation of mandatory administrative procedures for effective system security.	<p><b>MDN 04.16.10 - Added warnings to Section 3.1.1.4 and Section 3.1.1.4.4 indicating that counterfeit ballot detection is not supported in the current voting system release..</b></p>	<p><b>Accept 04/20/10 KA - Verified the ES&amp;S SHS DS200 Unity v. 3.2.1.0 REV 4.0 04/16/10, sections 3.1.1.4 and 3.1.1.4.4 still contains the content regarding the sensor. Warnings stating the counterfeit ballot detection is not supported in this release have been added to these sections.</b></p>
155	4/19/10	Sjakileti	Document Defect	Closed	Build Procedure DS200 FW v.1.4.3.1 Document v.1.2.1, 4/16/10	<p>The file name submitted in the DS200 build procedure is incorrect.</p> <p>DS200 build procedure file name is still showing v.1.4.3.0, instead of 1.4.3.1</p>	v.1: 8.5.a: The vendor shall establish such procedures and related conventions, providing a complete description of those procedures used to: Develop and maintain internally developed items;  EAC Voting System Testing and Certification Program Manual, v.1.0 Sec 5.5.1. Demonstrate that the software was built as described in the Technical Data Package.	<p><b>MDN 04.07.10 - DS200Firmware_BECI_v1.4.3.1_2010.04.16 Revised document provided with TDP Rev9a4.</b></p>	<p><b>Accept 0429/10 JG</b> Verified the document file name displays as v1.4.3.1 for "Build Procedure DS200 FW v.1.4.3.1 Document v.1.2.1 4/16/10"</p>
156	4/21/10	D. Valdez J. Garcia	Functional Defect	Closed	ERM 7.5.6.0	<p>An error occurs in ERM when uploading "Regular Precinct Results" with a System Type of "Mixed Mode".</p> <p>The WIOPRI Election is set to "Mixed Mode" in HPM. In the ERM SOP, pg. 94 it states if Mixed Mode is selected in HPM then the 650 group has two options to select "Absentee Precinct Results" OR "Regular Precinct Results". When reading in M650 results into ERM and selecting Regular Precinct Results, the following message was received, "WIOPRI.EC. Error 4702. Not open or</p>	v.1:2.2.1.b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.	<p><b>DZ 04.29.10 ERM SOP</b>- Added notes to section to "Update Absentee Precinct Results" and "Update Regular Precinct Results" stating that the results in question must come from the M650 Mixed Mode results disk and directing the user to the relevant sections of the HPM SOP where procedures for creating</p>	<p><b>Accept 05/03/10 JG -</b> Verified ES&amp;S ERM SOP Ver. Rel. 7.5.6.0 4/29/10 when creating an election in Mixed Mode AB and EC files are created. Depending on how the media is created (burning EC files or coping AB files) is how the uploading of results is determined. Absentee Precinct</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						wrong mode."		this disk are detailed.	Results is used for files ending in AB. Regular Precinct Results is used for files ending in EC.
157	4/21/10	Sjakileti	Document Defect	Closed	DS200 Sys Maint Manual, HW v.1.2.1.0, FW v.1.4.3.0, 4/9/10	<p>The SMM does not identify how to install DS200 from the CF card (Full Install).</p> <p>Procedures for copying the image to the CF card, using the COTS software Selfimage 1.2.1, are missing.</p>	v.2.2.8.3.a: The vendor shall provide specifications for validation of system installation, acceptance, and readiness. These specifications shall address all components of the system and all locations of installation (e.g., polling place central count facility), and shall address all elements of system functionality and operations identified in Section 2.3 above, including: Pre-voting functions	<b>BB05.07.10 - U3210_SMM00_DS200-</b> -- Added Ch 8, "Installing the DS200 Operating System."	<b>Accept 05/10/10 KA, SJ</b> Verified the DS200 Sys Maint Manual HW v.1.2.1.0 FW v.1.4.3.0 05/07/10 contains Ch 8 Installing the DS200 Operating System which includes directions on installing the DS200 operating system from a CF card using the COTS software Selfimage
158	4/29/10	J. Garcia	Informational	Closed	Jurisdiction Security Procedures ES&S v.1.0.0.1 5/8/08	A new JSP (Jurisdiction Security Procedures) document was submitted on 4/16/10 with the same previous version and release date. See discrepancy 134.		<b>MDN 05.04.10 - U3210_SSS01_JSP Template</b> -- Updated the cover date to reflect the date of revision (03.12.2010) and re-generated the PDF File.	<b>Accept 05/06/10 JG</b> Verified the JSP ES&S v.1.0.0.1 3/12/2010 was updated with the release date
159	5/5/10	J. Garcia	Document Defect	Closed	System Limitations Unity v. 3.2.1.0 dated 1/28/10 (precinct element)	<p>Inconsistencies on the precinct element limit.</p> <p>Under Unity System Limits section 1 it states "ERM report (65,535 on any precinct results import)" however, further down in this document it states, "65,500 (ERM limitation).</p>	V2: 2.3 The vendor shall provide a listing of the system's functional processing capabilities, encompassing capabilities required by the Standards and any additional capabilities provided by the system such as maximum # of precinct elements.	<b>MDN 05.07.10 U3210_OVR02_System Limitations</b> - Scaled the ERM Limitation in Section 1 to match the program limitation detailed later in the document. Both limits now consistently list 65,500 as the precinct element limit.	<b>Accept 05/10/10 KA</b> Verified the System Limitations Unity v.3.2.1.0 v. 8.0 3/9/10 is consistent on the precinct element limits and the ERM Limitation is shown as 65,500.
160	6/14/10	K.Wilson/ Sjakileti	Functional Defect	Closed	M100 Election V12S1, (ESS Unity 3.2.1.0 CRC-test-steps.xls)	<p>The externally modified M100 election definition was loaded on M100 without error.</p> <p>1. Modified election definition externally on PCMCIA card by replacing one bit in location 00008DBD(System Audit Log record), loaded election definition into</p>	2.1.2 d: Include control logic and data processing methods incorporating parity and checksums (or equivalent error detection and correction methods) to demonstrate that the system has been	<b>MDN 08.04.2010 -</b> Addressed with updated Model 100 Firmware (v5442). <b>GLW 06.23.10 - 1.</b> The CRC in the System Log Section is not validated by the M100 firmware	<b>2. Accept KGW &amp; SJ</b> 6/25/10--verified non-support of legacy data <b>1. Accept 8/12/10 SJ:</b> Modification in system audit log section of election definition is

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
						<p>M100, M100 accepted the election definition without any error.</p> <p>2. Modified election definition externally on PCMCIA card by replacing one bit in location 00008ED7(Scanning parameter section), loaded election definition into M100, M100 accepted the election definition without any error.</p> <p><b>1. Rejected 6/25/10 KGW &amp; SJ:</b> The argument that the system log records does not contain election results is rejected(this section contains the timestamp of Last polls Open) . If ERM cannot produce this log, and the originating M100 becomes inoperable, then the only recourse is that another M100 be able to read and produce this log. Failure to validate the CRC during such an operation fails the requirement for accuracy in producing log records.</p>	designed for accuracy	as this section contains no data structures that are significant election data or critical system events. Data that might be altered in this section will not effect the accuracy of the vote count or auditability of the key events during the election cycle. 2. As documented in the HPM, M100 and DS200 SDS documents, the Scanning Parameter Section is not longer used in this version of Unity and is only maintained for backwards compatibility for legacy tabulators. NOTE: The M100 does validate the CRC's stored in the following MCMCIA card / USB memory device PCB block sections: PCM Header Section, master Election Record, Counter Block Section and Audit Log Sections as alterations to data in these sections may effect the accuracy of the election results or ability to correctly audit the events of the election.	rejected by M100 FW v.5.4.4.2 displaying an error message "System audit log failed crc" and this message is printed	<b>1. Reject KGW &amp; SJ</b> 6/25/10
161	6/14/10	K.Wilson/Sjakileti	Functional Defect	Closed	DS200 (Election V12S1, ESS Unity 3.2.1.0 CRC-test-steps.xls)	<p>The externally modified DS200 election definition was loaded on the DS200without error.</p> <p>1. Modified election definition externally on USB by replacing one bit in location 00008DBD(System Audit Log record), loaded election definition into DS200, DS200 accepted the election definition without any error.</p>	2.1.2 d: Include control logic and data processing methods incorporating parity and checksums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy	<b>MDN 08.04.2010 -</b> Addressed with updated DS200 Firmware (v1433). <b>GLW 06.23.10 -</b> 1. The CRC in the System Log Section is not validated by the DS200 firmware as this section contains no data structures that	<b>1. Accept 8/11/10 SJ:</b> Modification in system audit log section of election definition is rejected by DS200 FW 1.4.3.3 displaying an error message "System audit log failed crc" and this message is printed	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
						<p>2. Modified election definition externally on USB card by replacing one bit in location 00008ED7(Scanning parameter section), loaded election definition into DS200, DS200 accepted the election definition without any error.</p> <p>1. 6/25/10 Rejected : The argument that the system log records does not contain election results is rejected(this section contains the timestamp of Last polls Open) . If ERM cannot produce this log, and the originating DS200 becomes inoperable, then the only recourse is that another DS200 be able to read and produce this log. Failure to validate the CRC during such an operation fails the requirement for accuracy in producing log records.</p>		are significant election data or critical system events. Data that might be altered in this section will not effect the accuracy of the vote count or auditability of the key events during the election cycle. 2. As documented in the HPM, M100 and DS200 SDS documents, the Scanning Parameter Section is not longer used in this version of Unity and is only maintained for backwards compatibility for legacy tabulators. NOTE: The DS200 does validate the CRC's stored in the following MCMCIA card / USB memory device PCB block sections: PCM Header Section, master Election Record, Counter Block Section and Audit Log Sections as alterations to data in these sections may effect the accuracy of the election results or ability to correctly audit the events of the election.	2. Accept KGW & SJ 6/25/10--verified non-support of legacy data  1. Reject KGW & SJ 6/25/10	
162	6/14/10	K.Wilson/Sjakileti	Functional Defect	Closed	DS200 (Election: V12S1, ESS Unity 3.2.1.0 CRC-test-steps.xls)	<p>DS200 USB- modified CRC was loaded into ERM without error.</p> <p>Scanned couple of ballots on the DS200, modified these results and loaded into ERM.</p> <p>1. Modified election results externally on USB by replacing one bit in location 00008DBD(System Audit Log record), loaded election results into ERM, ERM accepted the election results without any error.</p>	2.1.2 d: Include control logic and data processing methods incorporating parity and checksums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy	<b>MDN 08.04.2010 -</b> Addressed with updated DS200 Firmware (v1433). <b>GLW 06.23.10 - 1.</b> Altering data in the System Log Section does not modify election results as this section does not contain election results as documented in the	<b>2. Accept 6/25/10 KGW &amp; SJ -- verified non-support of legacy data</b> <b>3. &amp; 4. Accept 6/25/10 KGW &amp; SJ -- Since ERM doesn't read or produce these audit log records, the only recourse is for an DS200 to read and produce these records</b>	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<p>2. Modified election results externally on USB by replacing one bit in location 00008ED7(Scanning parameter section), loaded election results into ERM, ERM accepted the election results without any error.</p> <p>3. Modified election results externally on USB by replacing one bit in location 00009041(Audit Log Header Record ), loaded election results into ERM, ERM accepted the election results without any error.</p> <p>4. Modified election results externally on USB by replacing one bit in location 000090D9(Audit Log Records), loaded election results into ERM, ERM accepted the election results without any error.</p> <p>1. 6/25/10 Rejected: The argument that the system log records does not contain election results is rejected(this section contains the timestamp of Last polls Open) . If ERM cannot produce this log, and the originating DS200 becomes inoperable, then the only recourse is that another DS200 be able to read and produce this log. Failure to validate the CRC during such an operation fails the requirement for accuracy in producing log records.</p>		<p>HPM, M100 and DS200 SDS documents. ERM does validate the CRC's in the PCM Header Section, Election Definition Section and Counter Block Section as these are the only sections of data imported and then processed by ERM. 2. As documented in the HPM, M100 and DS200 SDS documents, the Scanning Parameter Section is not used by this Unity release and is only maintained for legacy tabulators. 3. ERM does not validate the CRC in the Audit Log Header Section as ERM does not import or process the Audit Log data from the M100 or DS200 tabulators. These Audit Logs must be printed on the applicable tabulator, which does validate the CRC's in the Audit Log Section. 4. ERM does not validate the CRC in the Audit Log Record Section as ERM does not import or process the Audit Log data from the M100 or DS200 tabulators. These Audit Logs must be printed on the applicable tabulator, which does validate the CRC's in the Audit Log Section. NOTE: ERM validates the CRC's in the PCM Header Section, master Election Record and Counter</p>	<p>during &amp; after an election during the archival period. Should the originating DS200 becomes inoperable, another DS200 must be capable of producing the audit records, since it is possible to close the polls and power down the DS200 without printing the audit log. The following tests are conducted to validate the ES&amp;S response :</p> <ul style="list-style-type: none"> <li>i. Verified that the voted (unmodified) election can be placed back into the DS200 and the DS200 will print the audit log records.</li> <li>ii. Verified that the DS200 can perform the previous operation in case the original DS200 from which the audit log was produced is inoperable or otherwise out of service during the archival period.</li> <li>iii. Verified that the DS200 refuses and reports a CRC error when given the modified header record cartridges that ERM accepted.</li> <li>iv. Verified that the DS200 refuses and reports a CRC error when given the modified audit records cartridges that ERM accepted.</li> </ul> <p>1. Reject 6/25/10</p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
								Block Section as altering data in these sections may effect the accuracy of the election results imported and processed into ERM.	KGW & SJ  Accept 8/11/10 SJ: 1. DS200 FW v.1.4.3.3 is able to validate the system audit log section, and able to produce this audit log.
163	6/14/10	K.Wilson/Sjakileti	Functional Defect	Closed	M100 (Election V12S1, s ESS Unity 3.2.1.0 CRC-test-steps.xls)	<p>M100 PCMCIA - modified CRC was loaded into ERM without error</p> <p>Scanned couple of ballots on the M100, modified these results and loaded into ERM:</p> <p>1. Modified election results externally on PCMCIA card by replacing one bit in location 00008DBD(System Audit Log record), loaded election results into ERM, ERM accepted the election results without any error.</p> <p>2. Modified election results externally on PCMCIA card by replacing one bit in location 00008ED7(Scanning parameter section), loaded election results into ERM, ERM accepted the election results without any error.</p> <p>3. Modified election results externally on PCMCIA card by replacing one bit in location 00009041(Audit Log Header Record ), loaded election results into ERM, ERM accepted the election results without any error.</p> <p>4. Modified election results externally on PCMCIA card by replacing one bit in location 000090D9(Audit Log Records), loaded election results into ERM, ERM accepted the election results without any error.</p> <p><b>1. Rejected 6/25/10:</b> The argument that the system log records does not contain election results is rejected(this section contains the timestamp of Last polls Open) . If ERM cannot produce this log, and the originating M100 becomes inoperable, then the only recourse is that another M100 be able to read and produce this log. Failure to validate the</p>	2.1.2 d: Include control logic and data processing methods incorporating parity and checksums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy	<b>MDN 08.04.2010</b> - Addressed with updated Model 100 Firmware (v5442).  <b>GLW 06.23.10</b> - 1. Altering data in the System Log Section does not modify election results as this section does not contain election results as documented in the HPM, M100 and DS200 SDS documents. ERM does validate the CRC's in the PCM Header Section, Election Definition Section and Counter Block Section as these are the only sections of data imported and then processed by ERM. 2. As documented in the HPM, M100 and DS200 SDS documents, the Scanning Parameter Section is not used by this Unity release and is only maintained for legacy tabulators. 3. ERM does not validate the CRC in the Audit Log Header Section as ERM does not import or process the Audit Log data from the M100 or DS200 tabulators. These Audit Logs must	<b>2. Accept 6/25/10</b> <b>KGW &amp; SJ</b> -- verified non-support of legacy data <b>3. &amp; 4. Accept 6/25/10</b> <b>KGW &amp; SJ</b> -- Since ERM does not read or produce these audit log records, the only recourse is for an M100 to read and produce these records during and after an election during the archival period. Should the originating M100 becomes inoperable, another M100 must be capable of producing the audit records, since it is possible to close the polls and power down the M100 without printing the audit log. The following tests are conducted to validate the ES&S response for these discrepancies: i. Verified that the voted (unmodified) election can be placed back into the M100 and the M100 will print the audit log records. ii. Verified that the M100 can perform the previous operation in case the original M100 from which the audit

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						CRC during such an operation fails the requirement for accuracy in producing log records.		be printed on the applicable tabulator, which does validate the CRC's in the Audit Log Section. 4. ERM does not validate the CRC in the Audit Log Record Section as ERM does not import or process the Audit Log data from the M100 or DS200 tabulators. These Audit Logs must be printed on the applicable tabulator, which does validate the CRC's in the Audit Log Section. NOTE: ERM validates the CRC's in the PCM Header Section, master Election Record and Counter Block Section as altering data in these sections may effect the accuracy of the election results imported and processed into ERM.	log was produced is inoperable or otherwise out of service during the archival period. iii. Verified that the M100 refuses and reports a CRC error when given the modified header record cartridges that ERM accepted. iv. Verified that the M100 refuses and reports a CRC error when given the modified audit records cartridges that ERM accepted.  <b>Accept 8/12/10 SJ:</b> 1.M100 fw 5.4.2.2 is able to validate the system audit log section, and able to produce this audit log. <b>1. Reject 6/25/10 KGW &amp; SJ</b>
164	7/6/10	S. Brown /K. Austin	Docu- ment Defect	Closed	Installing COTS: •ERM SOP Ver Rel 7.5.6.0 dated 5/3/10, HPM SOP Ver Rel 5.7.2.0 4/8/10, •OmniDrive USB/USB2 Installation Guide USB2 Driver V3.11 PC Card Manager V. 2.01 Doc Ver 1.0 5/20/08	Instructions to install an OmniDrive Parallel drivers are not provided.  The documentation specifically calls out the OmniDrive USB/USB2 Professional installation CD when installing the OmniDrive however, ES&S is also supporting OmniDrive Parallel. In order to use the OmniDrive USB/USB2 Professional installation CD for the OmniDrive Parallel the user must have the OmniDrive Parallel drivers. The documentation does not identify that the drivers have to be installed or how to obtain them. It is unclear to the user if it is proper to use the OmniDrive USB/USB2 Professional installation for the OmniDrive Parallel. Also the USB-USB Installation document does not contain the final steps of the PC Card Manager instructions or contain a	V2.2.4.2 The vendor shall provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for qualification testing.	DLZ 07.16.10 - ERM SOP Ch 5 and HPM SOP Ch 3 - Added the URL for the CSM support site where drivers for the serial OMNI Drive reader are staged.	Accept 07/20/10 SAB Confirmed HPM SOP, v.5.7.3.0, 7-16-10 & ERM SOP, v.7.5.7.0, 7-16-10 contain a note in the OmniDrive installation section with a link that takes the reader to the OmniDrive driver download website. While the instructions are still specifically for USB installation, they are similar in nature for the Parallel Port driver installation as found during testing. Installation is user-friendly and was successful with the

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						reference to their location in in the ERM and HPM SOP manuals.			correct driver.
165	7/26/10	S. Brown J. Garcia	Document Defect	Closed	ES&S DS200 SOP HW: v.1.2.1, Firmware v.1.4.3.3 06/30/10	<p>Calibration Counterfeit Ballot Sensor instructions are inconsistent</p> <p>In Ch 5 "Pre-Election Day Tasks" in Section "Calibrate Counterfeit Ballot Sensor" pg 50 a note at the top of the page states:</p> <p>"NOTE: If using the counterfeit ballot sensor run photocopies through the scanner to calibrate the sensor until the scanner will not accept the photocopies. If not using the counterfeit ballot sensor use your regular ballots to calibrate the scanner." Step #3 on pg 50 states for a user to insert a blank sheet of paper. The Note at the top of the page "If not using the counterfeit ballot sensor use your regular ballots" contradicts steps #3.</p>	V2.2.8.2a The vendor shall describe the system environment, and the interface between the user or operator and the system. .... A.Polling place	<b>DJZ 7-29-10 - Updated note now reads - NOTE: If using the counterfeit ballot sensor run photocopies through the scanner to test the sensor until the scanner will not accept the photocopies. If not using the counterfeit ballot sensor use your regular ballots to test the scanner."</b>	<b>Accept 08/03/10 SAB</b> Confirmed that DS200 SOP, FW v.1.4.3.3, July 30, 2010 has an updated Counterfeit Ballot section. The Calibrate Counterfeit Ballot Sensor section has been clarified. to identify when to use a blank sheet of paper to calibrate&ballots to confirm calibration.
166	7/26/10	J. Garcia	Document Defect	Closed	DS200 SMM HW V:1.2.1 FW V: 1.4.3.3 6/30/10	<p>The SMM does not identify how to install DS200 from the CF card (Full Install).</p> <p>Procedures for copying the image to the CF card, using the COTS software Self-image 1.2.1, are missing. This was Discrepancy 157 and it was closed with SMM HW 1.2.1.0 FW v.1.4.3.0 dated 05/07/10 containing Ch 8 "Installing the DS200 Operating System" however; Ch 8 has been removed in SMM HW 1.2.1 FW 1.4.3.3 6/30/10</p> <p>The May 7, 2010 version of this SMM document had instructions on how to create the DS200 O/S on the CF card in "Ch 8: Installing the DS200 Operating System". The July 30, 2010 version of this SMM document, Ch 7 discusses inserting the CF card into the DS200, but not creating it. There are no instructions in later steps on how to create this CF card either. These steps used to exist in the May 7, 2010 version of this System Maintenance Manual document.</p>	v.2.2.8.3.a: The vendor shall provide specifications for validation of system installation, acceptance, and readiness. These specifications shall address all components of the system and all locations of installation (e.g., polling place central count facility), and shall address all elements of system functionality and operations identified in Section 2.3 above, including: Pre-voting functions	<b>DJZ - 7-29-10 - Added Ch 7, "Install OS from Compact Flash" to the SMM.</b>  <b>DJZ - 8-6-2010 - Added in section for creating CF Card, in Ch 7 (pg 34)</b>	<b>Accept 8/09/10 JG SJ</b> Ch 7 of the SMM HW V: 1.2.1 FW V: 1.4.3.3 8/6/10 has been updated with the information to install OS from the Compact Flash.  <b>Reject 08/03/10 SAB</b>
167	7/26/10	J. Garcia	Document	Closed	DS200 SMM HW V:1.2.1	The SMM does not identify logic diagrams.	V2.2.9.2.2 The vendor shall provide	<b>DJZ - 7-29-10 - Added Ch 10, "Logic Diagrams"</b>	<b>Accept 08/03/10 SAB</b> Confirmed that FW

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
			Defect		FW V: 1.4.3.3 6/30/10	Logic diagrams were in SMM HW.1.2.1.0 FW v.1.4.3.0 dated 05/07/10 in Ch 10 however; Ch 10 "Logic Diagrams" has been removed in SMM HW 1.2.1 FW 1.4.3.3. 6/30/10	fault ... logic diagrams for all operation abnormalities identified by design and analysis and operation experience.	to the SMM.	v.1.4.3.3, 7/20/10 SMM, Ch 10 contains Logic Diagrams, as it did in the 5/7/10 document.
168	7/26/10	J. Garcia	Docu- ment Defect	Closed	DS200 SOP HW V:1.2.1 FW V: 1.4.3.3 7/16/10	Event 191 and 192 does not identify the action to be performed by the voter or pollworker  There are no "Text Messages" or "Numeric Messages" within the DS200 SOP that correspond with event numbers 191 or 192. The two new events (191 & 192) requires a voter or operator response however there is no documentation clarifying what action needs to be taken.	V2:2.8.5.a & c a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation c. Provides procedures that clearly enable the operator to intervene the system operations to recover from an abnormal system state. V1:2.2.5.2.2.e The message cue for all systems shall clearly state the action to be performed in the event that voter or operator response is required.	<b>DJZ 7-29-10</b> Updated message on pg 139 - Ballot found in scanner during startup is ejected <b>Cause:</b> Ballot is located in scanner at startup and is ejected. <b>Solution:</b> Press OK. Remove and reinsert the ballot  <b>Ballot found in scanner during startup can not be removed</b> <b>Cause:</b> Ballot is located in the scanner at startup but does not eject. <b>Solution:</b> Pull the DS200 forward and retrieve the ballot. Press OK. Push the DS200 back into place. If determination has been made that the ballot was not counted rescan the ballot. If the ballot was counted do not rescan the ballot, store it with the other counted ballots.	<b>Accept 08/03/10 SAB</b> Confirmed that FW 1.4.3.3, July 30, 2010 SOP, Ch 11, pg 139 now shows the two new messages as indicated that were added. Additionally, these messages are referenced on the Event Messages table on pg 164 that correspond to Event Numbers 191 and 192. Additionally, confirmed that 2 new numeric messages added - #140 and #141 as referenced in the Revision History. There are also two Warning messages similar in nature to #191 and #192 on pg 157-158.
169	8/3/10	S. Brown	Docu- ment Defect	Closed	Unity v.3.2.1.0, -Voting System Overview, 6/29/10 -SDS DS200, 7/1/10 -SFD DS200, 7/19/10 -SMM DS200, 6/30/10 -SOP DS200, 7/16/10	Documentation does not exist showing how to install the new ballot box deflectors as referenced in ECO665.  Review of these current 3.2.1.0 documents found no mention of the DS200 ballot box diverter extender field retro-fit (also called a deflector). The deflectors require specific placing and instructions for that placement do not exist.	V2:2.4.2 The vendor shall provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for qualification testing. The vendor shall provide a list of materials and components used in the system and a description of their assembly into	<b>MDN 08.04.2010</b> - Document titled Installation of the Extensions(rev2) .PDF includes instructions for installing ballot box deflectors. Submitted 8.6.2010 under the folder titled "U3210_DISC169_InstallInstructions."	<b>Accept 08/10/10 SAB</b> Confirmed that a new doc called Installation of the Extensions rev2 details how to add the diverter extensions, install and verify proper alignment of the deflectors. Pictures are provided each step

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
							major system components and the system as a whole.		
170	8/3/10	J. Garcia	Docu- ment Defect	Closed	DS200 SOP HW V:1.2.1 FW V: 1.4.3.3 July 16, 2010	The DS200 SOP document is missing samples of output reporting.  On Pg 77 Section "Print Election Reports" step 2 the documentation displays a list of Reports that can be printed once the Polls have been closed. The list is missing the "Poll Report Media" option. Also, it states "For descriptions and examples of each DS200 report, see Ch 9: Reports". There is no descriptions of Poll Reports in Ch. 9.	V2:2.8.2 The vendor shall describe the system environment and the interface between the user or operator and the system at the Polling Place or other locations. V2:2.8.4.a The vendor shall provide ... A detailed description of all input, output, control, and display features accessible to the operator. V2:2.8.4.c Sample data format and output reports	DJZ - 8-6-2010 - Added in Poll Report in Ch 9, (pg 124). The list on pg 77, does list the Poll Report Media currently.	Accept 08/09/10 JG Verified Ch 9 pg 126 of the DS200 SOP HW v. 1.2.1, FW v. 1.4.3.3 8/6/10 contains the Poll Report. DJZ/ESS is correct that Roll Report Media was not missing from the list. It's missing from a list on pg 124, however, the SOP clearly identifies that this is a report to run and how to display it.
171	8/3/10	J. Garcia	Docu- ment Defect	Closed	DS200 SOP HW V:1.2.1 FW V: 1.4.3.3 July 16, 2010	The DS200 SOP document is missing information on the Digital Table report pertaining to ballot diagnostics. In Ch 8 pg 87 in Section "Ballot Diagnostics" menu there is no information on the Digital Table report or a sample of the report.	V2:2.8.2 The vendor shall describe the system environment and the interface between the user or operator and the system at the Polling Place or other locations. V2:2.8.4.a The vendor shall provide ... A detailed description of all input, output, control, and display features accessible to the operator. V2:2.8.4.c Sample data format and output reports	DJZ - 8-6-2010 - Added Digital Table on Pg 88, in Ch 8, System Menus.	Accept 08/09/10 JG Verified Ch 8 pg 88 of the DS200 SOP HW v. 1.2.1, FW v. 1.4.3.3 8/6/10 identifies how to use the Digital Table reporting and provides a sample Digital Table report.
172	8/3/10	J. Garcia S. Brown	Func- tional Defect	Closed	DS200 System Maintenance Manual HW V:1.2.1 FW V: 1.4.3.3 July 30, 2010	The Documentation and the DS200 are inconsistent.  In Ch 8 on step 8 (pg. 43) it states: "Proceed With Update appears and a beeping noise will sound." however, there is no beeping noise.	V1:2.2.1.b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.	DJZ - 8-6-2010 - Removed "beeping noise will sound" in Ch 8 in SMM. Also removed same reference in SOP, which was in Ch 13, pg 183.	Accept 08/09/10 JG Verified in Ch 13 pg 187 DS200 SOP HW v. 1.2.1, FW v.1.4.3.3 8/6/10 & Ch 8 pg 43 of the SMM HW v. 1.2.1 FW v.1.4.3.3 8/6/10 the words "beeping noise will sound" are removed.
173	8/9/10	K. Swift	Docu- ment Defect	Closed	HPM SOP v.5.7.3.0 and ERM SOP v.7.5.7.0 both dated 7/16/10	The SOPs do not address that the M100Demo and control files, created during installation of HPM or ERM, need to be copied from C:elecdata to Q:elecdata after installation of either	V2:2.4.2 The vendor shall provide sufficient data, or references to data, to identify unequivocally the details of the system	MDN - 9.2.2010 - Updated the installation instructions included in HPM SOP (pg43) and the ERM SOP (pg 52) to	Accept 09/07/10 SAB Confirmed ERM &HPM SOP 9/3/10 were updated to include the required

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
						<p>HPM or ERM.</p> <p><b>Rejected 8/19/10 KA</b></p> <p>HPM SOP dated 7/16/10 pg 43 and ERM SOP dated 7/16/10 pg 52 state "if you need to copy files..." and "ES&amp;S recommends...". However, the files must be copied in order for the client server configuration to work. Also, the M100Demo and control files are not specifically mentioned. No new versions of the SOPs have been received.</p>	configuration submitted for qualification testing.	provide explicit instructions for moving control files when deploying HPM and ERM in a network environment. Control files are directly named. Updated documentation provided with TDP Rev JML - 8-17-2010 - HPM SOP pg 43 and ERM SOP pg 52 instruct the user to copy election files to the network as part of the installation.	steps for copying the control files from the local drive to the server \elecdata folder.  Reject 8/19/10 KA	
174	8/11/10	S. Brown K. Austin J. Garcia	Functional Defect	Closed	Mapping to Q and ERM 7.5.7.0 security Procedures settings	<p>ERM Security settings on a 2003 Server based network does not function properly.</p> <p>When logged into the Q drive and selecting ERM the user was not prompted to log in with 3 digit access. ERM opens and the user with restricted access now has full access. If one user had access to only display/scroll results they now have access to write back to the system. See Discrepancies 103 and 136.</p> <p><b>Rejected 8/19/10 KA</b></p> <p>Following the procedures in ERM SOP dated 7/16/10 pg 60-63 is not sufficient to set up the ERM Security Module. The discrepancy was written based on this version of the ERM SOP. No new version has been received.</p>	V2:2.2.5.3  Third, the system shall be configured to execute only intended and necessary processes during the execution of election software.  V1:6.5.6.b.1 The output file or database has no provision for write-access back to the system.	MDN - 9.2.2010 ERM SOP- Strengthened and clarified the ERM Security configuration section to require changing the path to the network control file. Following clarified instructions for network deployment under Ch 5 prevents the condition described in this discrepancy.	Accept 09/07/10 SAB Verified that steps added to the ERM SOP for #173, once the control files now make it possible to execute the steps on pg 60-63. Confirmed a new note has been added to change the default drive to the server drive (if needed) under step #5. Testing of the steps confirms ERM security works as documented	Reject 8/19/10 KA
175	08/17/10	Sjakileti	Source code	Closed	DS200 1.4.3.3e source code  Unity 3.2.1.0 System Change Notes, Revision 11.0	All pointers have not been reset to Null as identified in BUG18361 & ENH18269  Found 2 instances not resetting the pointer used to free allocated memory to a "Null" state after memory is freed. 1. DS200 1.4.3.3e\Source\TouchScreen\Src\xf86Elo.c, Line 1606.	v2:5.4.2e : Pointers or which provide for specifying absolute memory locations, provides controls that prevent the pointer or address from being used to overwrite executable instructions or to access		Accept 8/23/10 SJ: Verified by code review that DS200 1.4.3.4b addresses resetting pointers to NULL	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						2. DS200 1.4.3.3e\Source\AppLegacy\Src\Shared.c, Line 587	inappropriate areas.		
176	08/24/10	S. Brown K. Austin J. Garcia	Document Defect	Closed	HPM SOP v.5.7.3.0 and ERM SOP v.7.5.7.0 both dated 7/16/10	<p>ERM SOP 7.5.7.0 and HPM SOP 5.7.3.0 do not address what additional re-hardening steps that need to be performed for software updates.</p> <p>The documentation identifies steps to uninstall the ERM and HPM but it does not explicitly identify what portions of the Hardening Procedures are required to successfully install an updated version of the software. address the scenario of installing. There is no reference to Post Application Install script and steps .</p>	V2.2.4.2 The vendor shall provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for qualification testing. The vendor shall provide a list of materials and components used in the system and a description of their assembly into major system components and the system as a whole.	MDN - 9.2.2010 - Updated section 13.1 of the Hardening Procedures for the Election Management PC document (U3210_SSS02_HardeningProcedures) with a warning requiring re-executing the post-install hardening script after re-installing any election management	<p>Accept 09/08/10 SAB Confirmed a warning appears in section 13.1 of the Hardening procedure 9/2/10 "If you uninstall and reinstall any EMS application, you must re-run the PostInstall.exe hardening script after you finish re-installing election software." A warning sufficient to alert users to required actions when the program is uninstalled and reinstall is provided in the Post-install instructions.</p>
177	9/20/10	K. Wilson	Functional Defect	Closed	DS200 v.1.4.3.4b IFCA DS200 Func TC modem-counterfeit Rev00 step 4)	<p>Code does not contain functionality to record the modem status in the audit log</p> <p>Reviewed source code did not contain an audit log event report that indicates the absence or presence of a modem following a hardware diagnostics tests performed at startup or prior to opening the polls.</p> <p><b>9/27/10 CEC Reject</b> The EAC had concerns that untested code was being submitted in ENH14728. As identified in the 9/9/10 call with ESS and iBeta, iBeta is to review the submitted code as a protection beyond the 3.2.0.0 disabling of the modem. EAC instructions clarifying the scope of 3.2.1.0 are found in section 2.1.6 of v.6.0 of the test plan.</p>	<p>V1.2.2.1.e Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation</p> <p>f. Incorporate a means of implementing a capability if access to a system function is to be restricted or controlled</p> <p>V1.4.4.2.a Prior to the start of ballot counting, a system process shall verify hardware and software status and generate a readiness audit record. This record shall include the identification of the software release, the identification of the election to be processed,</p>	<p>SMP - 9.23.2010 - Identical to the <u>ESSUnity3200</u> voting system, certified by the EAC on July 21, 2009, moderning is not supported in the 3.2.1.0 release. Please reference EAC July 21, 2009 Agence Decision - Grant of Certification letter, ES&amp;S Unity 3.2.0.0 Certificate of Conformance July 21, 2009, and iBeta Unity 3.2.0.0 VSTL Certification Test Report, Version 3.0 discrepancy #135 acceptance clarification statement. It is unclear why additional requirements are applicable to this</p>	<p>Accept 11/12/10 SJ &amp; JG</p> <p>The DS200 FW v.1.4.3.7 displays modem status in initial state Report and Audit Log.</p> <p>10/22/10 CEC - KW confirmed in code review that a check for the modem and report to the audit log is included in v.1.4.3.6c.</p> <p><b>9/27/10 CEC Reject</b></p>

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
							<i>and the results of software and hardware diagnostic tests.</i>	<i>release. It is our belief the conditions regarding the modem exclusion from Unity 3.2.0.0 also apply to Unity 3.2.1.0.</i>		
178	9/20/10	K. Wilson	Document Defect	Open	Voting System Overview Unity v.3.2.1.0 3/24/10  System Security Spec Ver. Rel.3.2.1.0 4/16/10  DS200 System Ops Pro HW v.1.2.1 FW v.1.4.3.4 3/27/10  HPM Sys Ops Proc Ver. Rel.5.7.3.0 9/3/10	While the disclaimer at the front of various TDP documents contains a statement disallowing the use of "remote transmission," there are no statements clarifying that the certified system does not have and cannot have a modem installed to maintain its EAC certification. Based on source code review, the installation of a modem and the existence of a telephone number in the ballot definition would allow the DS200 to transmit vote counts over public telecommunications systems after the polls are closed. This activity could occur without any identification or authentication of the persons performing the activity and could occur automatically if the ballot definition is so configured. No procedural or technical controls were found to prevent the installation of a modem in the DS200.  <b>9/27/10 CEC Reject</b> <b>The EAC had concerns that untested code was being submitted in ENH14728. As identified in the 9/9/10 call with ESS and iBeta, iBeta is to review the submitted code as a protection beyond the 3.2.0.0 disabling of the modem. EAC instructions clarifying the scope of 3.2.1.0 are found in section 2.1.6 of v.6.0 of the test plan</b>	V2:2.4.2 The vendor shall provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for testing. The vendor shall provide a list of materials and components used in the system and a description of their assembly into major system components and the system as a whole. Paragraphs and diagrams shall be provided that describe: ... Operator and voter safety considerations, and any constraints on system operations or the use environment  V1:2.2.1.e Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation  f. Incorporate a means of implementing a capability if access to a system function is to be restricted or controlled	SMP - 9.23.2010 - Identical to the ESS Unity 3.2.0.0 voting system, certified by the EAC on July 21, 2009, modeming is not supported in the 3.2.1.0 release. Please reference EAC July 21, 2009 Agence Decision - Grant of Certification letter, ES&S Unity 3.2.0.0 Certificate of Conformance July 21, 2009, and iBeta Unity 3.2.0.0 VSTL Certification Test Report, Version 3.0 discrepancy #135 acceptance clarification statement. It is unclear why additional requirements apply to this release. It is our belief the conditions regarding the modem exclusion from Unity 3.2.0.0 apply to Unity 3.2.1.0.	<b>9/27/10 CEC Reject</b>	
179	09/23/10	D. Valdez	Informational	Closed	ES&S Configuration Mgmt Plan Unity 3.2.1.0 v. 3.0 section 9.7.1.	ECO format was not consistent with the CM Plan example.  In the QA and CM Spot Check an electronic copy or image of the completed Engineering Change Order (ECO) was requested for comparison to the CM documentation . The ECO			Accept 09/23/10, DV: The example provided in the CM Plan represented an ECO format used by Pivot, but ECOs can be generated from different entities s;	

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						provided did not match the information in the ES&S Configuration Management Plan Unity 3.2.1.0 v. 3.0 section 9.7.1.			Verified the CM Plan, sect. 9.7.1 & 9.7.2, differentiate between Pivot generated ECO forms and ES&S generated ECO forms. The ECO was consistent with the updated CM Plan.
180	09/23/10	D. Valdez	Informational	Closed	ES&S Configuration Mgmt Plan Unity v. 3.2.1.0 v.3.0 3/10/10, pg 38 sec 4.3.1	<p>Approval process was not consistent with the CM Plan process description.</p> <p>In the QA and CM Spot Check a screen shot of the ECO 841 tracking was requested to check for approval of release to the VSTL. The screen shot of the E-Synergy process flow for ECO 841 did not show evidence of SVP systems and Project Office approval as documented in the CM Plan Unity 3.2.1.0 v.3.0 section 4.3.</p>			Accept 09/23/10, DV: Verified E&S updated their CM Plan, sections 4.3.1, 4.3.2.2, and the ECO Policies and Procedures v.2.0 to clarify HW system changes and ECOs do not require specific approval from the SVP Systems for release to the VSTL. ECOs entered into E-Synergy for tracking are approved.
181	10/6/10	K. Wilson	Document Defect	Open	DS200 System Ops Proc HW v.1.2.1 FW v.1.4.3.4 3/27/10 SWDesign Spec DS200 Unity v.3.2.1.0 8/24/10	<p>Error code is not listed in the specifications.</p> <p>The errno, errno_, "System Error Number" or E value is reported by the DS200 audit log or printed tape for error events. This is a C runtime error code. Values and corresponding errors for this code do not appear in the TDP.</p>	<p>V2:2.5.6.1.c . For each software function or operating mode, the vendor shall provide: ... c. A definition of the outputs produced (again, with characteristics, tolerances, or acceptable ranges as applicable).</p> <p>V2:2.5.6.2.d The vendor shall describe the software's capabilities or methods for detecting or handling: Error logging for audit record generation;</p> <p>V2:2.5.7.2.e e. If the software module or unit contains, receives, or outputs data, a description of its inputs, outputs, and other data elements as applicable.</p>		
182	10/08/	K. Wilson	Docu-	Open	DS200 System	DS200 documentation of unrecoverable	V.2:2.2.1.d & f: The		

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
10			ment Defect		Dps Proc HW v.1.2.1 FW v.1.4.3.4 3/27/10  SW Design Spec DS200 Unity v.3.2.1.0 3/24/10	<p>system errors and the scanner interface is insufficient.</p> <p>Unrecoverable system errors from the DS200 scanner are identified in the SOP (Numeric messages). The unrecoverable System Errors (Event # 203, 205, 210-217, Numeric Messages 103, 105, 110-117) are not sufficiently detailed in the TDP. The "Cause" for each item states, "The scanner encountered an unrecoverable error in the operating system". The solution identified is similar, although not identical verbiage, except for the statement, "Do not use the scanner again until an ES&amp;S technician repairs the DS200". The interface to the DS200 scanner over which these errors traverse is not identified in the SDS document.</p> <p>Note: 11/5/10 -- SDS updated to v8.0 11/4/10 -- These errors are now marked in the SDS as being "Reserved for future use" The SOP updated to 9/17/10 (no version) has no change in the "Numeric Messages" section of Ch 11, and the "Audit Log Messages" table is now inconsistent with the one in the SDS. Furthermore, in reference to the "traverse" in the original discrepancy, there is no explanation in the SDS that errors received from the scanner are in the 200+ range and that these errors are translated down to the 100+ values that appear in "Numeric Messages" section. In the SOP Table under "Audit Log Messages" and in the SDS Table under "Audit Log Messages" the 200+ values appear with the corresponding 100+ value in parenthesis. However nowhere does it describe the relationship between these values and how they will appear on the display of the audit log in the 100+ range but in the audit log itself, as well as the two previously described "Audit Log Messages" tables they appear in the 200+ range (see set_err_msg in scan.c).</p>	<p>system description shall include written descriptions, drawings and diagrams that present:</p> <ul style="list-style-type: none"> <li>d. Descriptions of the functional and physical interfaces between subsystems and components;</li> <li>f. Interfaces among internal components, and interfaces with external systems. For components that interface with other components for which multiple products may be used, the TDP shall provide an identification of:</li> </ul> <ol style="list-style-type: none"> <li>1) File specifications, data objects, or other means used for information exchange; and</li> <li>2) The public standard used for such file specifications, data objects, or other means;</li> </ol> <p>V.2.2.5.6.2 a &amp; b: The vendor shall describe the software's capabilities or methods for detecting or handling:</p> <ul style="list-style-type: none"> <li>a. Exception conditions;</li> <li>b. System failures;</li> </ul>		

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						Current TDP does not satisfy v.2: 2.2.1.f:"file specifications ... used for information exchange"			
183	10/18/10	J. Garcia	Functional Defect	Closed	M100 5.4.4.3 (Clearing total)	<p>When in the L&amp;A test mode a message appears stating "Clear Election Test Results and Leave Election Test Menu?" If he user selects NO the totals are still being zeroed.</p> <p>1. Go to the Diagnostic-Test menu &amp; select ELECTION TEST; on the Election Test menu &amp; select TEST BALLOT, on the Ballot Test menu &amp; select FEED BALLOTS.</p> <p>2. Scan 4 ballots. Go to Reports and print Poll Report.</p> <p>3. Select the PREVIOUS button 3 times.</p> <p>4. Message "Clear Election Test Results and Leave Election Test Menu? YES/NO" appears. Select NO</p> <p>5. The message "Counters are set to Zero.... OK" appears. OK is the only option to get out and the totals were zeroed.</p>	<p>V1:2.3.4 Election personnel conduct equipment and system readiness tests prior to the start of an election to ensure that the voting system functions properly, f. Segregating test data from actual voting data; either procedurally or by hardware/software features.</p> <p>V1:2.2.8.1. Software modules required to: b. Accommodate device control functions performed by polling place officials ...</p> <p>V1:2.2.1. b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.</p>	20101108 MDN - Addressed with DS200 version 1.4.3.7	Accept 11/4/10 KS: Verified in 3210 Regression test case, step 1, with M100 FW: 5.4.4.4, that the totals are not being zeroed when selecting 'No'.
184	10/20/10	K. Wilson	Functional Defect	Closed	DS200 v1.4.3.6c  step 3 of Security Test v6	<p>Error_hdl does not address all scenarios associated with a full audit log. (reference add_event in pcm.c).</p> <p>If the audit log is nearly full (has 2 slots left), and if an event not originating from error_hdl flows into add_event, the resulting audit log will have 2 entries "AUDIT LOG FULL" and the original event will not make it into the audit log because the seek will fail as the audit log is now full. This result is a change in behavior from v1.4.3.4b and earlier versions because of the global nature of the logging done in error_hdl.</p>	V1:2.2.4.1.i. Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator; and	20101108 MDN - Addressed with DS200 version 1.4.3.7	Accept 11/16/10 KW verified v.1.4.3.7 does not continue to scan ballots after the audit log is full and reports that the audit log is full without losing the event precipitating that message. No events are lost when the audit log is full.
185	10/25/10	J Garcia Sjakileti	Functional Defect	Closed	DS200 v1.4.3.4  Audit Log Full  step 3 of Security Test v6	<p>DS200 did not halt after a critical system failure (Audit Log Full)</p> <p>iBeta manipulated the "Audit Log entry" within the PCB file to an artificially low number in order to test reaching the</p>	V1:2.1.5.2 The system shall also be configured to halt election software processes upon the termination of any critical system process (such as	20101108 MDN - Addressed with DS200 version 1.4.3.7	Accept 11/16/10 KW Verified v.1.4.3.7 does not continue to scan ballots after the audit log is full and reports that the audit log is full

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						maximum number of log entries. After opening the polls and scanning two ballots a message displayed "Audit Log Full.....". The tester scanned multiple ballots after the message. They were accepted without an error or issue and the ballot counter incremented. The "Audit Log Full" message never reappeared. The DS200 did not halt after the critical system failure (Audit Log Full). The audit log was printed and only displayed the events prior to the Audit Log Full message. All scanned ballots were recorded in the totals.	system audit) during the execution of election software. V1.2.2.5.2.1.d The audit record shall be active whenever the system is in an operating mode. V1.2.2.5.1 Election audit trails provide the supporting documentation for verifying the accuracy of reported election results. They present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation.		without losing the event precipitating that message. No events are lost when the audit log is full.
186	11/3/10	J Garcia SJakileti	Functional Defect	Closed	DS200 PM FW update	The updated Power Management firmware (PM FW) version was displayed even though the DS200 generated an error and the installation failed.  During installation of a firmware update the DS200 was not plugged in properly and the battery was low. A full install was completed via the CF card. While attempting to install the upgrade a message appeared on the screen stating that the install was not successful. The error was not written to the tape and the tape did not print the successful installation confirmation. The DS200 powered down. After plugging in the DS200 the unit was powered back up. The Initial State Report incorrectly displayed the updated PM FW version as the current firmware version on the machine. There was no indication that the software update failed or was successful. The state of the unit was unknown. In a subsequent review of the source code it was found that there was	2005 v.1:2.1.1. b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.	20101108 MDN - Addressed with DS200 version 1.4.3.7	Accept 11/17/10 JG and SJ DS200 FW v.1.4.3.7 verified that a failed upgrade provides the user with an error prior to shutting down and during power up. This message is printed the paper tape. Upon start up the message allows the user to restart the FW upgrade or shutdown.

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
						<i>no provision beyond the screen message to check the state, advise the user or record the failure. (Installation of the firmware is outside the election audit log functionality, because there is not election on the machine during an installation.)</i>			
187	11/11/10	C Coggins J Garcia	Functional Defect	Open	DS200 v.1.4.3.7 Cross vote alert	<p>Ballot reported as returned to voter was dropped in the bin without incrementing the counter.</p> <p>Ballot #2, was the second cross voted ballot in the test election. It was inserted in the DS200 scanner; "You have cross voted" appeared on the screen; "Accept" was selected by the tester; the ballot dropped into the bin but the counter failed to increment. A screen message flashed indicating there was an issue with the ballot. A second message flashed that the ballot was being returned. Two ballots in the ballot box and one ballot recorded on the counter were observed. The polls were closed. The audit log reported the "Ballot Removed During Scan (137)". The cross over vote report did not report the second ballot as either accepted or rejected.</p>	<p>2005 v.1: 2.1.1 .b To ensure security all systems shall: provide system functions that are executable in the intended manner or order, and only under the intended conditions.</p> <p>v.1: 2.1.2 .c To ensure vote accuracy, all systems shall: record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast.</p> <p>v.1: 2.1.8.b For all voting systems each piece of voting equipment that tabulates ballots shall provide a counter that: records the number of ballots cast during a ... election.</p>		
188	11/11/10	Kelly Swift & J. Garcia	Functional Defect	Open	M100 v.5.4.4.4 Audit Logs	<p>M100 did not write to the audit log after changing the date.</p> <p>When the System Setting Date Time, was changed there was not entry in the audit log .</p>	RFI 2009-04 & 2.1.4.g Record and report the date and time of normal and abnormal events.		
189	11/11/10	K. Wilson/Sj akileti	Functional Defect	Open	DS200 v.1.4.3.7 Shutdown Loop  (Security TC Step 6)	<p>The counter block CRC failure and shutdown button contain a loop.</p> <p>DS200, v1.4.3.7. Modified the CRC of the counter block of a voted election and attempted to restart and reopen the polls. During startup, the DS200 reports a "COUNTER BLOCK FAILED CRC" error on the screen and paper tape. The screen presenting this error contains a shutdown button. Pressing the shutdown</p>	V1:2.2 This section defines required functional capabilities that are system-wide in nature and not unique to pre-voting, voting, and post-voting operations. All voting systems shall provide the following functional capabilities: ... • Error recovery;		

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation	
						button causes the DS200 to display a printing message and the CRC error is printed again. Then the DS200 returns to the same screen displaying a "COUNTER BLOCK FAILED CRC" error. In observing this result, the shutdown button was pressed a total of 3 times. This behavior is an infinite loop with no way to shutdown the DS200 as displayed. After the third observation that the shutdown button failed to perform its function, the memory cartridge compartment was unlocked and the power button was held down. The DS200 displayed the screen with the query to continue with shutdown. When the "Continue with Shutdown" button was pressed the DS200 did shut down.	V2:2.8.5.c. Provides procedures that clearly enable the operator to intervene the system operations to recover from an abnormal system state;			
190	11/11/10	K. Wilson/Sjakileti	Functional Defect	Open	DS200 v.1.4.3.7 Audit Log (Security TC Step 6)	Audit log does not record a printer-time out event.  While testing for the audit log full, prior to opening the polls of an election, the paper tape was low and was replaced with a fresh roll. The paper tape was slightly misaligned and the zero report was not printing. The access door to the power button was unlocked and opened and the printer compartment was unlatched. At that point the display showed a printer time-out. The tape was corrected and the test step was restarted. When the audit log was printed as a normal course of the test step, the event of a printer time-out did not appear.	V1:2.2.4.1... All Systems shall ... g. Record and report the date and time of normal and abnormal events; V1:2.2.5.1 [Audit trails] present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation. RFI 2009-04			
191	11/11/10	J Garcia	Document Defect	Open	SMM HW v.1.2.1; FW v. 1.4.3.6; 9/17/10 Check the Battery Charge SOP FW v.1.4.3.6 9/17/10 Battery Charge Indicator	The System Maint. Manual and SOP are displaying the Battery Charge indicator/check inconsistently.  The SOP displays the Battery Charge Indicators however: the SMM displays a photo and text that does not correctly reflect the DS200 functionality.	V2:2.9 The system maintenance procedures shall provide information in sufficient detail to support election workers, systems personnel, or maintenance personnel in the adjustment or removal and replacement of components....			
192	11/19/10	J Garcia Sjakileti	Functional Defect	Open	DS200 FW 1.4.3.7 Continue on	The DS200 the "continue on battery only" option functions inconsistently.	V1:2.2.1.b. Provide system functions that are			

#	Date	Tester	Type	Status	Location	Issue Description	Standard- Requirement	Vendor Response	Validation
					Battery Backup	After powering up on battery back up power , a message displays "No Main Power Detected" the user selects "continue on battery only" button. If the unit has an election installed the Admin Password screen is displayed instead of the "Election Definition Found" screen. If no election is present the "Election Definition Not Found" screen is displayed.	executable only in the intended manner and order, and only under the intended conditions.		

## ***7.6 Appendix F: Warrant of Accepting Change Control Responsibility***

This statement is provided by ES&S when certification testing is completed.

## 7.7 Appendix G: Trusted Build & Validation Tools Unity 3.2.1.0 voting system

The ES&S Unity 3.2.1.0 voting system is composed of the hardware, software, and documents identified in [section 3 Voting System Identification](#). This section documents the final trusted builds performed in Unity 3.2.1.0 testing. Builds that were not changed from **ESSUNITY3200** are documented in Appendix G of the **ESSUNITY3200** Test Report.

iBeta uses a COTS hash program (Maresware) to obtain File Size, MD5 and SHA1 hashes during all witnessed and trusted builds. Algorithms have been validated using the test data from the NIST NSRL website (<http://www.nsrl.nist.gov/testdata/>). This program is widely used in forensic analysis of systems and also used by some states to verify their voting software. The MD5 and SHA1 hashes are taken to be consistent with currently distributed NSRL data files which contain the hash resulting from each of those algorithms. Listed below are the Source Code Applications reviewed by iBeta for the tested Trusted Builds and Witness of the Unity 3.2.1.0 voting system firmware and software. (NIST Handbook 150-22 4.2.3, 4.13.2, 4.13.4, 5.10.4 VSS vol. 1: 9.6.2.4)

### 7.7.1 Witness of the Trusted Build of ERM v. 7.5.7.0, HPM v.5.7.3.0 and MYDLL v1.1.0.2

Application/ Component	Version	Language	File Signature
ERM	7.5.7.0a	COBOL	ERM7.5.7.0_HPM5.7.3.0_MYDLL1.1.0.2_TBSource_06172010.hash.txt
HPM	5.7.3.0b	COBOL	ERM7.5.7.0_HPM5.7.3.0_MYDLL1.1.0.2_TBSource_06172010.hash.txt
MYDLL	1.1.0.2c	C	ERM7.5.7.0_HPM5.7.3.0_MYDLL1.1.0.2_TBSource_06172010.hash.txt

Document Prior to the Trusted Build:	
Vendor Name	ES&S 3.2.1.0
Vendor Consultant(s) (5.6)	Dave Herrera
Witness Name (5.6)	Sridevi Jakileti
Witness Title	Trusted Builder
Vendor Build Document(s) used and version(s)	<p>Build Procedure Unity 3.2.1.0 Election Management System (EMS) Build 4 .Document Version 1.2 ,6/16/2010</p> <p>Below documents are not used directly in the current build, because build environment is restored from 05212009_PostCOTS Ghost Image from the <b>ESSUNITY3200</b> build</p> <ul style="list-style-type: none"> <li>WinXP-CorsairwithVGA_INST_2009.04.22.pdf</li> <li>Visual Studio_6.0_EntEdwithSP5_INST_2009.04.30.pdf</li> <li>vbAdvance3.1_INST_2009.04.30.pdf</li> <li>VisualStudio2005ProEd_INST_2009.04.21.pdf</li> <li>RMCOBOLDeveloper11.01_INST_2009.04.29.pdf</li> <li>AvocetADXZ180_INST_2009.04.30.pdf</li> <li>Codebase6.5Release3_INST_2009.04.21.pdf</li> <li>CrystalReports9_INST_2009.04.29.pdf</li> <li>PCCardSDKv2.20_INST_2009.04.30.pdf</li> <li>Xerces2.7.0_INST_2009.04.25.pdf</li> <li>InstallShieldPro7.01_INST_2009.03.23.doc</li> <li>InstallShieldExpress2.1_INST_2008.11.30.pdf</li> </ul>
Equipment Used	<p>SLOT3 Corsair Orbit, S/N 1112719, 2.8 GHz, Pentium 4, 1 Gb RAM, Windows XP SP3 (same as Unity 3.2.0.0 build)</p>
ibeta COTS used to clean the build environment disk (name and version) (5.6.1.1)	Restored from post cots image from Unity3.2.0.0 TB05212009 (Unity3.2.0.0_PostCOTS_05212009.GHO)
iBeta COTS used to generate HASH file signatures (name and version)	Mares Hash Ver. 07.08.10.07.12
Construct the build environment (5.6.1.2)	
Verify (by signature) that the build environment is isolated and controlled by	Sridevi Jakileti

iBeta	
Witness attests to verifying that the source code being built is the source code provided by iBeta	Sridevi Jakileti
Vendor CM Tool and version	HPM: Microsoft Visual SourceSafe 6.0(product version) 6.0.93.50 (File Version - Client) ERM: Microsoft Visual SourceSafe 6.0(product version) 6.0.93.50 (File Version - Client)
Build Environment Operating System	Windows XP with Service Pack 3
Build tool(s) and version(s)	<b>Audit Manager:</b> Microsoft Visual Studio 2005 <b>ALL other unity software:</b> Visual Studio 6.0 Enterprise with Service Pack 5 <b>ERM and HPM:</b> RM/COBOL v11.01
3 <sup>rd</sup> Party Libraries and Version	<b>ESSZIP:</b> zip32.lib; unzip32.lib, <b>Audit Manager:</b> asyfilt.dll2.40.4275.1, Comcat.dll, comct332.ocx6.7.0.8988, comdlg32.ocx6.0.84.18, msado25.tlb2.5 2.60.6526.0, msadodc.ocx6.0.88.4, msbind.dll6.0.88.62, mscreun.dll6.0.88.4 mscomct2.ocx 6.0.88.4, mscomctl.ocx 6.0.88.62, msderun.dll6.0.88.4, msflxgrd.ocx6.0.84.18, msvbvm60.dll6.0.89.64, oleaut32.dll2.40.4275.1, olepro32.dll5.0.4275.1, stdole2.tlb2.40.4275.1, sysinfo.ocx6.0.81.69, vb6stkit.dll 6.0.84.50, comct332.ocx 6.7.0.8988, comdlg32.ocx6.0.84.18, msadodc.ocx6.0.88.4, mscomct2.ocx6.0.88.4, mscomctl.ocx6.0.88.62, msflxgrd.ocx6.0.84.18, sysinfo.ocx6.0.81.69, msbind.dll6.0.88.62, mscreun.dll6.0.88.4, msderun.dll6.0.88.4, msrdo20.dll6.0.88.62, msstdfmt.dll6.0.88.4, rdocs.dll6.0.88.4, <b>ESSIM:</b> mfc80.dll8.0.50727.42, mfc80u.dll8.0.50727.42, mfcm80.dll8.0.50727.42, mfcm80u.dll8.0.50727.42, msbcm80.dll8.0.50727.42, mstcp80.dll8.0.50727.42, msvcr80.dll8.0.50727.42, msvcr71.dll8.0.50727.42, msvcrt.dll6.0.8797.0, roboex32.dll9.20.534.0, unzip32.dll5.5.2.0, zip32.dll 2.3.1.0, microsoft.vc80.crt.manifest, microsoft.vc80.mfc.manifest, <b>EDM :</b> c4dll.dll1.0.0.1, crdb_p2bxbsse.dll9.2.1.106, crpe32.dll9.2.3.745, crqe.dll9.2.1.605, crttslv.dll9.2.0.528, crxf_pdf.dll9.2.1.567, crxf_rtf.dll9.2.0.566, crxf_wordw.dll9.2.0.566, crxf_xls.dll9.2.1.662, exportmodeller.dll9.2.1.559, inetwh32.dll7.0.133.0, msver71.dll7.10.3052.4, roboex32.dll9.0.79.0, u2ddisk.dll9.2.0.541, u2ftext.dll9.2.1.555, ufmanager.dll9.0.0.1, xerces-c_2_7.dll2.7.0.0 <b>ERM:</b> ROBOEX32.DLL 8.0.131.0,wh2robo.dll13.10.606.6, asyfilt.dll2.40.4275.1, comcat.dll4.71.1460.1, comct332.ocx6.7.0.8988, comdlg32.ocx6.0.84.18, mscomct2.ocx6.0.88.4, mscomctl.ocx6.0.88.62, MSVBVM50.DLL5.1.43.19, msvbvm60.dll6.0.89.64, mstcp60.dll6.0.8168.0, MSVCRTD.DLL5.0.0.7022, oleaut32.dll2.40.4275.1, olepro32.dll5.0.4275.1, OpenSaveFile.ocx1.0.0.0, RICHTX32.OCX6.0.88.4, stdole2.tlb2.40.4275.1, sysinfo.ocx6.0.81.69, tabctl32.ocx6.0.90.43, WSC32.DLL0.0.0 Linker Rev. 3, WSC32.lib, <b>HPM:</b> HtmIWH.dll7.0.131.0, ROBOEX32.DLL8.0.133.0, asyfilt.dll2.40.4275.1, comcat.dll4.71.1460.1, omct332.ocx6.7.0.8988, comdlg32.ocx6.0.84.18, MFC42D.DLL6.0.8447.0, mscomct2.ocx6.0.88.4, mscomctl.ocx6.0.88.62 ,msdxm.ocx6.4.9.1128, msvbvm60.dll6.0.89.64, mstcp60.dll6.0.8168.0, MSVCP60D.DLL6.0.8168.0, msver70.dll6.0.8797.0, MSVCRTD.DLL6.0.8447.0, oleaut32.dll2.40.4275.1, olepro32.dll5.0.4275.1, OpenSaveFile.ocx1.0.0.0, Quartz.dll6.4.2600.1221, RICHTX32.OCX6.0.88.4, stdole2.tlb2.40.4275.1

3 <sup>rd</sup> Party Source Code (COTS) and Version	Codebase 6.5, Release 3 Modified COTS Codebase file - d4all.h
3 <sup>rd</sup> Party DLLs, Drivers, etc. and Version(s)	Windows XP with Service Pack 3, MicroVisual Studio 2005 Visual Studio 6.0 Enterprise with Service Pack 5 Yong Dynamic Software vbAdvance 3.1 RM/COBOL v11.01 Compiler RM/COBOL v11.01 WOW Extensions 64180 macro assembler version 4.01a by 2500 A.D. Software Crystal Reports 9 Full Developer Crystal Reports 9 Main Program Files Patch (05/14/2003) Crystal Reports 9 Database and Export Patch (05/14/2003) OmniDrive SDK v1.01 Sourceforge Info-Zip Zip version 2.32 Source forge Info-Zip Unzip version 5.52 Xerces-C 2.7.0 Install Shield Professional version 7.01 Install Shield Express version 2.1
Additional file(s) loaded and version(s)	Codebase file - d4all.h (Modified COTS) Build Scripts and Executables from previous trusted build are loaded with source code. <b>Build Scripts from 6/17/2010</b> – (BuildScripts.ini, ESSInstallFileList.txt, ESSPreBuiltFileList.txt, ESSScriptFileList.txt, ESSSourceFileList.txt, TB-0_CheckInputMedium.bat, TB-2_LoadSourceCode.bat, TB-3_CreateExecutables.bat, unzip.exe, TB-2_LSC-0.1_SetEnvironmentVariables.bat, TB-2_LSC-0.2_MakeDirectories.bat, TB-2_LSC-0.3_CreateLoadLog.bat, TB-2_LSC-1_ERMExecutable.bat, TB-2_LSC-2_ERMInstall.bat, TB-3_CE-0.01_SetEnvironmentVariables.bat, TB-3_CE-0.02_CreateBuigLog.bat, Tb-3_CE-1.01_ERMExecutable.bat, TB-3_CE-2.01_ERMInstall.bat, Tb-0_CIM-0_SetEnvironmentVariables.bat) <b>Executables from previous Trusted build_05212009:</b> - (Init650.exe, serve650.exe, vioWin.exe, VioDialog.exe, UndrVote.exe, ShellSetup.exe, Shell.exe, RegUtil.dll, RegUtil.lib, pbmtobmp.exe, mydll.dll, mydll.lib, MPRBoot.HEX, Images.exe, makelbin.exe, HPMDLL.dll, HPMDLL.lib, GetAuditData.exe, ExitWin.exe, Events.exe, ESSPEB.dll, ESSPEB.lib, ESSPEB.h, ESSPCMIO.dll, ESSPCMIO.lib, ESSM100.dll, ESSM100.lib, ESSEAGL.dll, ESSEAGL.lib, ESSEAGL.h, ESSCRYPT1.DLL, ESSCRYPT1.lib, BlowFish.h, BlowFishDll.h, ERMDLL.dll, ERMDLL.lib, CRCDLL.dll, CRCDLL.lib, cb_rand.dll, cb_rand.lib, cf_utility.exe, cb_peb.dll, cb_peb.lib, cb_m100.dll, cb_m100.lib, cb_eagl.dll, cb_eagl.lib, CB_650.DLL, CB_650.lib) These are loaded with the source code CD
Record the disk image software version being used	Norton GHOST V:11.0
Record the filename of the build environment file signature (5.6.1.3) –	Unity3.2.0.0_PostCOTS_05212009.hash.txt
Record the filename of the build environment disk image –	Restored from post cots image from Unity3.2.0.0 TB05212009 (Unity3.2.0.0_PostCOTS_05212009.GHO)
Verify (by signature) the build environment file signature (5.6.1.3)	Sridevi Jakileti
<b>Loading Source Code (5.6.2)</b>	
Record the file signature of the source code (5.6.2.1)	see table of source code, above
Verify (by signature) that each file signature of the source code loaded matches as documented above (5.6.2.1)	Sridevi Jakileti
Method of Build Witness	Trusted Build

Record the combined source code and pre-build environment file signature (5.6.2.2)	Unity3.2.1.0_PreBuild_ERM_HPM_MYDLL_06172010.hash.txt
Record the combined source code and pre-build environment disk image (5.6.2.3)	PreBuild_ERM_HPM_MYDLL_06172010.GHO
Record the Final Build Version – Unique Identifier	ERM 7.5.7.0, HPM5.7.3.0, MyDLL 1.1.0.2
Certification Application Number (if applicable)	ESS0703
<b>Document during the Build Witness:</b>	
Date / Time Build Initiated	6/17/2010 11.10am
Compiler and Version	<p><b>ERM:</b> WOW Extensions Designer version 11.01, RM/Cobol for Windows version 11.01, RM/Cobol Code bridge for Windows, Microsoft Visual C++ 6.0, Borland C/C++ 5.01, Microsoft Visual Basic 5.0, Install Shield Express 2.12</p> <p>Build environment is restored from the PostCots_05212009 ghost image, below build tools and compiler are used in the current build.</p> <p><b>HPM:</b> Cobol-WOW version 3.12, RM/Cobol for Windows version 7.50.01, RM/Cobol Code bridge for Windows, Microsoft Visual C++ 6.0, Borland C/C++ 5.01, Microsoft Visual Basic 5.0, Install Shield Express 2.12</p> <p><b>EDM:</b> Microsoft Visual Studio 6.0 SP 5, Install Shield Professional 7.01</p> <p><b>Audit Manager and ESSIM:</b> Microsoft Visual Basic 6.0 SP6, Install Shield Professional 7.01</p>
Application Name	Unity3.2.1.0 ERM, HPM, MYDLL
Application Version Order	ERM7.5.7.0, HPM5.7.3.0, MyDLL1.1.0.2
Obtain Names and Signatures of all persons present during build (record below)	SJakileti, Dave Herrera
Issue(s) and Resolution(s)	No Issues
<b>Document at Completion of the Build Witness:</b>	
Record the disk image of the final build (5.7.3)	PostBuild_ERM_HPM_MYDLL_06172010.GHO
Record file signature of the final build (5.6.3.1)	Unity3.2.1.0_PostBuild_ERM_HPM_MYDLL_06172010.hash.txt
Record the type of unalterable storage media being used for installation disk(s) (i.e., CD) – (5.6.3.2)	CD, NAS2
Record each piece of media that is part of the installation disk (each must have a unique identifier) (5.6.3.2, 5.7.5)	Trusted Build ERM7.5.7.0 and HPM 5.7.3.0 installs_06172010
Record the file signature of the installation disk(s). (5.6.3.3, 5.7.5) (include in below archive)	Unity3.2.1.0_ERM7.5.7.0_HPM5.7.3.0_TBInstalls_06172010.hash.txt
Record the type of unalterable storage media being used for pre-build and post-build archive disk (i.e., CD) –	NAS2
Record each piece of media that is part of the pre-build archive disk (each must have a unique identifier) (5.6.2.4, 5.7.2, 5.7.3)	NAS2
Explanation of any significant differences observed	No differences

### 7.7.2 Witness of the Trusted Build of M100 v. 5.4.4.4

Application/ Component	Version	Language	File Signature
M100	5.4.4.4.1	C	M1005.4.4.4.1_TBSOURCE_11042010.hash.txt

Document Prior to the Trusted Build:	
Vendor Name	ES&S 3.2.1.0
Vendor Consultant(s) (5.6)	Dave Herrera
Witness Name (5.6)	Sjakileti
Witness Title	Trusted Builder
Vendor Build Document(s) used and version(s)	Build Procedure Model 100 Precinct Tabulator firmware Version 5.4.4.4, version1.0, October 29,2010  QNX4.22_INST_2009.08.14.pdf
Equipment Used	Dell Optiplex G110 S/N: 20PW10B
iBeta COTS used to clean the build environment disk (name and version) (5.6.1.1)	restored from image M100_postCOTS_09032009.GHO
iBeta COTS used to generate HASH file signatures (name and version)	SLAX 5.1.8 Live W/SHA1DEEP and MD5DEEP
Construct the build environment (5.6.1.2)	
Verify (by signature) that the build environment is isolated and controlled by iBeta	Sridevi Jakileti
Witness attests to verifying that the source code being built is the source code provided by iBeta	Sridevi Jakileti
Vendor CM Tool and version	Concurrent Versions System (CVS) 1.11.2 (client/server)
Build Environment Operating System	QNX 4.22A Operating System
Build tool(s) and version(s)	<b>M100 Firmware:</b> QNX/Sybase Watcom C Compiler version 10.6
3rd Party Libraries and Version	QNX 4.22A Operating System QNX 4.22 Manual Patch Disk QNX/Sybase Watcom C Compiler version 10.6 QNX Product Suite May 2001 Upgrade QNX Embedded Kit version 1.0 QNX Embedded Kit version 1.0 Manual Patches: Efsys.386ex, Efsys.cirrus, boot.386exp, commons.lib, compress.o, cstart_copy.o, cstart_ram.o, nocis.o, sss.lib, xip.o QNX 4.22A Embedded Licenses: qnx0063793n001, tcprt0097975n001
3rd Party Source Code (COTS) and Version	None
3rd Party DLLs, Drivers, etc. and Version(s)	None
Additional file(s) loaded and version(s)	Unity 3.2.1.0 Model 100 version 5.4.4.4.1 Source and Build Scripts CD with:  M100 Build scripts: ce-m100.sh lsc-m100.sh scripts.ini  M100 Source: buildpkg.tar source.tar
Record the disk image software version being used	Norton GHOST V:11.0
Record the filename of the build environment file signature (5.6.1.3) –	M100_PostCots_09222009.hash M100_PostCots_Sha1_09222009.hash

Record the filename of the build environment disk image –	M100_postCOTS_09032009.GHO
Verify (by signature) the build environment file signature (5.6.1.3)	Sridevi Jakileti
<b>Loading Source Code (5.6.2)</b>	
Record the file signature of the source code (5.6.2.1)	see table of source code, above
Verify (by signature) that each file signature of the source code loaded matches as documented above (5.6.2.1)	Sridevi Jakileti
Method of Build Witness	Trusted Build
Record the combined source code and pre-build environment file signature (5.6.2.2)	M1005.4.4.4_PreBuild_MD5_11042010.hashl M1005.4.4.4_PreBuild_SHA1_11042010.hashl
Record the combined source code and pre-build environment disk image (5.6.2.3)	M1005.4.4.4_PreBuild_11042010.GHO
Record the Final Build Version – Unique Identifier	M100 5.4.4.4
Certification Application Number (if applicable)	ESS0703
<b>Document during the Build Witness:</b>	
Date / Time Build Initiated	11/4/2010 10.20 am <b>Note:</b> System time in the QNX system is GMT. MST is GMT-7, so all Ghost and Hash files will have a datetime stamp of 7 hours ahead of the actual time they were generated.
Compiler and Version	<b>M100:</b> QNX/Sybase Watcom C Compiler version 10.6
Application Name	M100 Firmware
Application Version Order	5.4.4.4
Obtain Names and Signatures of all persons present during build (record below)	Sridevi Jakileti, Dave Herrera
Issue(s) and Resolution(s)	See Notes
<b>Document at Completion of the Build Witness:</b>	
Record the disk image of the final build (5.7.3)	M1005.4.4.4_PostBuild_11042010.GHO
Record file signature of the final build (5.6.3.1)	M1005.4.4.4_PostBuild_MD5_11042010.hashl M1005.4.4.4_PostBuild_SHA1_11042010.hashl
Record the type of unalterable storage media being used for installation disk(s) (i.e., CD) – (5.6.3.2)	CD
Record each piece of media that is part of the installation disk (each must have a unique identifier) (5.6.3.2, 5.7.5)	Trusted Build M1005.4.4.4_11042010 Installs
Record the file signature of the installation disk(s). (5.6.3.3, 5.7.5) (include in below archive)	M1005.4.4.4_TBInstall_11042010.hash.txt
Record the type of unalterable storage media being used for pre-build and post-build archive disk (i.e., CD) –	NAS2 drive
Record each piece of media that is part of the pre-build archive disk (each must have a unique identifier) (5.6.2.4, 5.7.2, 5.7.3)	NAS2 drive
Explanation of any significant differences observed	No Issues

### 7.7.3 *Witness of the Trusted Build of DS200 v. 1.4.3.7*

Application/Component	Version	Language	File Signature
DS200	1.4.3.7a	C/C++	DS2001.4.3.7a_TBSOURCE_11082010.hash.txt

<b>Document Prior to the Trusted Build:</b>	
Vendor Name	ES&S
Vendor Consultant(s) (5.6)	Sue McKay
Witness Name (5.6)	Sridevi Jakileti
Witness Title	Trusted Builder
Vendor Build Document(s) used and version(s)	Build Procedure DS200 Firmware version 1.4.3.7, version1.1 ,November 8,2010
Equipment Used	Dell #E085 Slot1
iBeta COTS used to clean the build environment disk (name and version) (5.6.1.1)	Restored from DS200 TOS PostBuild (DS200TOS_PostBuild_07202010.GHO) as a Build environment for DS200 Firmware
iBeta COTS used to generate HASH file signatures (name and version)	Mares Hash Ver. 07.08.10.07.12
<b>Construct the build environment (5.6.1.2)</b>	
Verify (by signature) that the build environment is isolated and controlled by iBeta	Sridevi Jakileti
Witness attests to verifying that the source code being built is the source code provided by iBeta	Sridevi Jakileti
Vendor CM Tool and version	Concurrent Versions System (CVS) 1.11.22
Build tool(s) and version(s)	Linux From Scratch 6.25
Build Environment Operating System	Linux operating system 6.25
3 <sup>rd</sup> Party Libraries and Version	Please see build procedure DS200 Target Operating System (TOS) Version1.0.2.0, Document Version 1.0,June25,2010
3 <sup>rd</sup> Party Source Code (COTS) and Version	None
3 <sup>rd</sup> Party DLLs, Drivers, etc. and Version(s)	Please see build procedure DS200 Target Operating System (TOS) Version1.0.2.0, Document Version 1.0,June25,2010
Additional file(s) loaded and version(s)	Used BuildScripts of DS200 1.4.3.7 (BuildFirmware1.sh, BuildFirmware2.sh, BuildFirmware3.sh, VersionNumbers.txt), PMB.hex (1.2.0.1, built 5/28/2009) coming from 3.2.0.0_DS200AncillaryDevices (trusted Build) fw.iic (2.20.0.0) coming from 3.2.1.0_DS200AncillaryDevices trusted Build )
Record the disk image software version being used	Norton GHOST V:11.0
Record the filename of the build environment file signature (5.6.1.3) –	DS200TOS1.0.2.0_PostBuild_07202010.hash.txt
Record the filename of the build environment disk image –	DS200TOS_PostBuild_07202010.GHO
Verify (by signature) the build environment file signature (5.6.1.3)	Sridevi Jakileti
<b>Loading Source Code (5.6.2)</b>	
Record the file signature of the source code (5.6.2.1)	see table of source code, above
Verify (by signature) that each file signature of the source code loaded matches as documented above (5.6.2.1)	Sridevi Jakileti
Method of Build Witness	Trusted Build
Record the combined source code and pre-build environment file signature (5.6.2.2)	DS2001.4.3.7_PreBuild_11082010.hashl
Record the combined source code and pre-build environment disk image (5.6.2.3)	DS2001.4.3.7_PreBuild_11082010.GHO
Record the Final Build Version – Unique Identifier	DS200 1.4.3.7
Certification Application Number (if applicable)	ESS0703
<b>Document during the Build Witness:</b>	
Date / Time Build Initiated	11/08/2010 1.20pm

Compiler and Version	GCC-4.0.3 (GNU Compiler Collection). This compiler is part of the LFS (Linux From Scratch) 6.2-5 Live CD
Application Name	DS200
Application Version Order	Ds200 1.4.3.7
Obtain Names and Signatures of all persons present during build (record below)	Sridevi Jakileti, Sue McKay
Issue(s) and Resolution(s)	No Issues
<b>Document at Completion of the Build Witness:</b>	
Record the disk image of the final build (5.7.3)	DS2001.4.3.7_PostBuild_11082010.GHO
Record file signature of the final build (5.6.3.1)	DS2001.4.3.7_PostBuild_11082010.hashl
Record the type of unalterable storage media being used for installation disk(s) (i.e., CD) – (5.6.3.2)	CD
Record each piece of media that is part of the installation disk (each must have a unique identifier) (5.6.3.2, 5.7.5)	Trusted Build DS200 1.4.3.7_11082010 Installs
Record the file signature of the installation disk(s). (5.6.3.3, 5.7.5) (include in below archive)	DS2001.4.3.7_TBInstalls_11082010.hash.txt
Record the type of unalterable storage media being used for pre-build and post-build archive disk (i.e., CD)	Nas2
Record each piece of media that is part of the pre-build archive disk (each must have a unique identifier) (5.6.2.4, 5.7.2, 5.7.3)	Nas2
Explanation of any significant differences observed	No Issues

#### 7.7.4 *Witness of the Trusted Build of DS200 Ancillary v. 2.20.0.0*

Application/ Component	Version	Language	File Signature
Scanner C8051	2.20.0.0.a	C	DS200AncillaryInputTB_12292009.src.hash.txt

<b>Document Prior to the Trusted Build:</b>	
Vendor Name	ES&S
Vendor Consultant(s) (5.6)	Dave Herrera
Witness Name (5.6)	Kevin Wilson, Alastair Mayer
Witness Title	Trusted Builder
Vendor Build Document(s) used and version(s)	WinXPwithSP3-DellOptiplexGX520_INST_2009.03.31.pdf IAREmbeddedWorkbench3.40_INST_2009.04.20.pdf KeiluVision3DevelopmentTools4.2007_INST_2009.04.20.pdf CypressEZ-USBReferenceDesignKit2.31_INST_2009.04.20.pdf DS200AncillaryDevices_BECI_3.2.1.0_2009.12.15.pdf
Equipment Used	DellOptiplexGX520
iBeta COTS used to clean the build environment disk (name and version) (5.6.1.1)	Active KillDisk for DOS V4.1 Build 2380
iBeta COTS used to generate HASH file signatures (name and version)	Mares Hash Ver. 07.08.10.07.12
<b>Construct the build environment (5.6.1.2)</b>	
Verify (by signature) that the build environment is isolated and controlled by iBeta	Kevin Wilson
Witness attests to verifying that the source code being built is the source code provided by iBeta	Kevin Wilson
Vendor CM Tool and version	Concurrent Versions System (CVS) 1.11.22
Build Environment Operating System	Windows XP Professional Version 2002 Service Pack 3

Build tool(s) and version(s)	eil µVision3 Development Tools Cypress CY4611 EZ-USB FX2 Reference Design Kit IAR Embedded Workbench EW430
3 <sup>rd</sup> Party Libraries and Version	As below
3 <sup>rd</sup> Party Source Code (COTS) and Version	As below
3 <sup>rd</sup> Party DLLs, Drivers, etc. and Version(s)	As below
Additional file(s) loaded and version(s)	Build scripts(unzip.exe, TB-3_CreateExecutables.bat, TB-2_LoadSourceCode.bat, TB-0_CheckInputMedium.bat, ESSSourceFileList.txt, ESSScriptsFileList.txt, BuildScripts.ini, TB-2_LSC-2_ScannerBoard.bat, TB-2_LSC-1_PowerManagementBoard.bat, TB-2_LSC-0.2_MakeDirectories.bat, TB-2_LSC-0.1_SetEnvironmentVariables.bat, TB-3_CE-0.01_SetEnvironmentVariables.bat, TB-3_CE-1.01_PowerManagementMsp430.bat, TB-3_CE-1.02_ScannerC8051.bat, TB-0_CIM-0_SetEnvironmentVariables.bat)
Record the disk image software version being used	Norton GHOST V:11.0
Record the filename of the build environment file signature (5.6.1.3) –	DS200Ancillary_PostCots_05282009.hash.txt
Record the filename of the build environment disk image –	DS200Ancillary_PostCots_05282009.GHO
Verify (by signature) the build environment file signature (5.6.1.3)	Kevin Wilson
<b>Loading Source Code (5.6.2)</b>	
Record the file signature of the source code (5.6.2.1)	see table of source code, above
Verify (by signature) that each file signature of the source code loaded matches as documented above (5.6.2.1)	Kevin Wilson
Method of Build Witness	Trusted Build
Record the combined source code and pre-build environment file signature (5.6.2.2)	DS200Ancillary_PreBuild_12292009.hash.txt
Record the combined source code and pre-build environment disk image (5.6.2.3)	DS200Ancillary_PreBuild_12292009.GHO
Record the Final Build Version – Unique Identifier	Scanner C8051 2.20.0.0
Certification Application Number (if applicable)	ESS0703
<b>Document during the Build Witness:</b>	
Date / Time Build Initiated	12/29/2009 8:45 am MST (PC set to CST 7:45)
Compiler and Version	See Build tools and versions
Application Name	DS200ancillary Devices (Scanner)
Application Version Order	2.20.0.0
Obtain Names and Signatures of all persons present during build (record below)	Kevin Wilson, Alastair Mayer Dave Herrera
Issue(s) and Resolution(s)	No Issues
<b>Document at Completion of the Build Witness:</b>	
Record the disk image of the final build (5.7.3)	DS200Ancillary_PostBuild_12292009.hash.txt
Record file signature of the final build (5.6.3.1)	DS200Ancillary_PostBuild_12292009.GHO
Record the type of unalterable storage media being used for installation disk(s) (i.e., CD) – (5.6.3.2)	NAS2
Record each piece of media that is part of the installation disk (each must have a unique identifier) (5.6.3.2, 5.7.5)	DS200Ancillary install files are (fw.iic) input to DS200 firmware build on NAS2 ESS Unity 3.2.1.0\Unity3.2.1.0_TrustedBuild\Unity 3.2.1.0_DS200_TrustedBuild_2009Dec29\ds200_stage_Ancillary_12 292009
Record the file signature of the installation disk(s). (5.6.3.3, 5.7.5) (include in below archive)	DS200Ancillary_Archive_12292009.hash.txt
Record the type of unalterable storage media being used for pre-build and post-build archive disk (i.e.,	NAS2

CD)	
Record each piece of media that is part of the pre-build archive disk (each must have a unique identifier) (5.6.2.4, 5.7.2, 5.7.3)	NAS2\ESS Unity 3.2.1.0\Unity3.2.1.0_TrustedBuild\Unity 3.2.1.0_DS200_TrustedBuild_2009Dec29
Explanation of any significant differences observed	No differences

### 7.7.5 Witness of the Trusted Build of AutoMARK VAT v. 1.3.2097

Application/ Component	Version	Language	File Signature
VAT	1.3.2097a	VB.Net	04132010_AutoMark_VAT_1.3.2097a.hash.txt

Document Prior to the Trusted Build:	
Vendor Name	ES&S
Vendor Consultant(s) (5.6)	Dave Herrera
Witness Name (5.6)	Alastair Mayer, Sridevi Jakileti
Witness Title	Trusted Builder
Vendor Build Document(s) used and version(s)	ES&S AutoMARK(i) VAT 1.3.2907 Software and Firmware Compilation Instructions , 4/9/2010
Equipment Used	Dell Optiplex GX520
iBeta COTS used to clean the build environment disk (name and version) (5.6.1.1)	Restored the unity3.2.0.0 PreBuild image (ESS_AutoMark_PreBuild_05272009.GHO)
iBeta COTS used to generate HASH file signatures (name and version)	Mares Hash Ver. 07.08.10.07.12
Construct the build environment (5.6.1.2)	
Verify (by signature) that the build environment is isolated and controlled by iBeta	Alastair Mayer
Witness attests to verifying that the source code being built is the source code provided by iBeta	Dave Herrera
Build Environment Operating System	Windows XP Professional Version 2002 Service Pack 2
Vendor CM Tool and version	None
Build tool(s) and version(s)	VAIO System Recovery DVD PCG-K23/PCG-K25/PCG-K27 Series Microsoft Embedded Visual C++ 4.0 Service Pack 4. Microsoft Visual Studio .NET 2003 Service Pack 2 Keil Software µVision2, C compiler Version 2.40 Texas Instruments Code Composer Studio. Version 2.0 Cosmic Compiler V 4.1H Borland C 4.02 Prog08sz Programmer for v 2.05 Atmel Flip v2.4.6 Atmel MCU ISP Software V1.0 Microsoft Access XP/2002 InstallShield 10.5 Microsoft Windows CE With Platform Builder Version 5.0
3 <sup>rd</sup> Party Libraries and Version	ACCESSRT.MSI v2002,MSOHELP.exe 10.0.2609.0,Office1.cab v2002, OSP.MSI v2002,OSP1.cab v2002,FILES\SYSTEM\EXTRACT.exe v2002, FILES\SYSTEM\MLANG.DAT v2002,FILES\SYSTEM\MLANG.DLL 5.0.2919.6304,FILES\SYSTEM\MSXML.DLL 5.0.2919.6303, FILES\SYSTEM\T2EMBED.DLL,0.2.0.69,FILES\WINDOWS\HELP\OS.HLP v2002,IE5\EN\ACTSETUP.cab v2002,IE5\EN\ADVAUTH.cab v2002, IE5\EN\AOLSUPP.cab v2002,IE5\EN\AXA.cab v2002,IE5\EN\AXA2.cab v2002,IE5\EN\AXA3.cab v2002,IE5\EN\BRANDING.cab v2002, IE5\EN\DCOM95.exe 4.71.1015.0,IE5\EN\DXDDEX.cab v2002,IE5\EN\DXMINI.cab v2002,IE5\EN\FONTCORE.cab v2002,

	IE5\EN\FONTSUP.cab v2002,IE5\EN\FPESETUP.cab v2002, IE5\EN\GSETUP95.cab v2002,IE5\EN\GSETUPNT.cab v2002, IE5\EN\HELPCONT.cab v2002,IE5\EN\HHUPD.cab v2002, IE5\EN\ICW.cab v2002,IE5\EN\ICWCON.cab v2002, IE5\EN\IE4MFC40.cab v2002,IE5\EN\IE4SHL95.cab v2002, IE5\EN\IE4SHLNT.cab v2002,IE5\EN\IE5COMP.exe 5.0.2919.6307 IE5\EN\IE5SETUP.exe 5.0.2919.6307,IE5\EN\IECIF.cab v2002, IE5\EN\IEDATA.cab v2002,IE5\EN\IEDATAJA.cab v2002, IE5\EN\IELPKAD.cab v2002,IE5\EN\IELPKAR.cab v2002, IE5\EN\IELPKIW.cab v2002,IE5\EN\IELPKJA.cab v2002, IE5\EN\IELPKKO.cab. v2002,IE5\EN\IELPKPE.cab v2002, IE5\EN\IELPKTH.cab v2002,IE5\EN\IELPKVI.cab v2002, IE5\EN\IELPKZHC.cab v2002,IE5\EN\IELPKZHT.cab v2002, IE5\EN\IENT_S1.cab v2002,IE5\ENIENT_S2.cab v2002, IE5\EN\IENT_S3.cab v2002,IE5\ENIENT_S4.cab v2002, IE5\EN\IENT_S5.cab v2002,IE5\ENIESETUP.INI v2002, IE5\EN\IE_EXTRA.cab v2002,IE5\EN\IE_S1.cab v2002, IE5\EN\IE_S2.cab v2002,IE5\EN\IE_S3.cab v2002, IE5\EN\IE_S4.cab v2002,IE5\EN\JAAIME.cab v2002, IE5\EN\KOAIME.cab v2002,IE5\ENMAILNEWS.cab v2002, IE5\EN\MDAC_IE5.cab v2002,IE5\EN\MOBILE95.cab v2002, IE5\EN\MOBILENT.cab v2002,IE5\EN\MPDCDS.cab v2002, IE5\EN\MPPLAYER2.cab v2002,IE5\EN\MSN_AUTH.cab v2002, IE5\EN\NM30.cab v2002,IE5\ENOAINST.exe 4.71.1015.0 IE5\EN\SCAIME.cab v2002,IE5\EN\SETUPNT.cab v2002, IE5\EN\SETUPW95.cab v2002,IE5\EN\SWDIR.cab v2002, IE5\EN\SWFLASH.cab v2002,IE5\EN\TCAIME.cab v2002, IE5\EN\TS95.cab v2002,IE5\EN\TSNT.cab v2002, IE5\EN\USP10.cab v2002,IE5\EN\VBSCRIPT.cab v2002, IE5\EN\VGX.cab v2002,IE5\EN\VMX86_01.cab v2002, IE5\EN\VMX86_02.cab v2002,IE5\EN\VRML2C.exe 4.71.1015.0 IE5\EN\WAB.cab v2002,IE5\EN\WEBFLDRS.cab v2002, IE5\EN\WPIE5X86.cab v2002,chs.syn 6.1.0.0 chsrom.DLL 6.1.0.0,eci.DLL 6.1.0.0,enu.syn 6.1.0.0 esm.syn 6.1.0.0,jpn.syn 6.1.0.0,jpnrom.DLL 6.1.0.0 kor.syn 6.1.0.0,korrom.DLL 6.1.0.0,ARIALUNI.TTF,BATANG.TTF MSMINCHO.TTF,PMINGLIU.TTF,sqlxml.MSI c3.0 xblkld3.DLL 3.30.3457.0,Helper.exe,SqlRun.cab,,SqlRun01.MSI 1033dotnetfx.exe 1.1.4322.573 1033,dotnetfxSp1.exe 1.0.0.0,dotnetfxSp1.exe 1.0.871.2738 chs.syn v6.1.0.0,chsrom.DLL v6.1.0.0,eci.DLL v6.1.0.0, enu.syn v6.1.0.0,esm.syn v6.1.0.0,jpn.syn v6.1.0.0, jpnrom.DLL v6.1.0.0, kor.syn v6.1.0.0,korrom.DLL v6.1.0.0,chs.syn v6.1.0.0, chsrom.DLL v6.1.0.0, eci.DLL v6.1.0.0,enu.syn v6.1.0.0,esm.syn v6.1.0.0, FTD2XX.DLL v6.1.0.0, ftd2xx.inf v6.1.0.0,ftdi_d2xx.DLL v6.1.0.0,jpn.syn v6.1.0.0,jpnrom.DLL v6.1.0.0,kor.syn v6.1.0.0,korrom.DLL v6.1.0.0,Microsoft.WindowsCE.Forms.DLL v1.0.2268.0, MSCORLIB.DLL v1.0.2268.0,regflush.exe System.DATA.Common.DLL 1.0.2268.0,ICSharpCode.SharpZipLib.DLL 0.85.1.271,New Text Document.txt 0.85.1.271,SharpZipLib_0855_Bin[1].zip 0.85.1.271,cabwiz.ddf,Cabwiz.exe 3.1.0.9386,CFResGen.exe 1.0.4128.0, Makecab.exe, unzip.exe 5.52, WinCEPB50-060430-2006M04-Armv4I.msi V5.0,WinCEPB50- 060831-2006M08-Armv4I.msi V5.0,WinCEPB50-060228-2006M02- Armv4I.msi V5.0,WinCEPB50-060131-2006M01-Armv4I.msi V5.0,WinCEPB50-060731-2006M07-Armv4I.msi V5.0,WinCEPB50- 060630-2006M06-Armv4I.msi V5.0,WinCEPB50-060331-2006M03- Armv4I.msi V5.0, WinCEPB50-060531-2006M05-Armv4I.msi V5.0,WinCEPB50- 041231-Product-Update-Rollup-Armv4I.msi V5.0,WinCEPB50-
--	--

	051231-Product-Update-Rollup-Armv4I.msi V5.0, autoit-v3-setup.exe 3.3.0.0, ADS_XSCALE_4_2_SDK.msi, DATA.TAG v2.4.6,data1.cab v2.4.6, lang.dat v2.4.6,layout.bin v2.4.6, os.dat v2.4.6,setup.bmp v2.4.6, SETUP.EXE v2.4.6,SETUP.INI v2.4.6, setup.ins v2.4.6,setup.lid v2.4.6, _INST32I.EX_ v2.4.6,_ISDEL.EXE v2.4.6, _setup.dll v2.4.6,_sys1.cab v2.4.6, _user1.cab v2.4.6,evc4sp4.exe v4 PL2303.CAT,SER2PL.INF,SER2PL.SYS DISK.INI v7.09,c51util.dll v7.09,TX51TNY.LIB v7.09,CONF_TNY.A51 v7.09,DBG_TINY.DSW v7.09, GENRTX.BAT v7.09,READ.ME2 v7.09, RIGHT.A51 v7.09,RTX51TNY.A51 v7.09, VERS.A51 v7.09,
3 <sup>rd</sup> Party Source Code (COTS) and Version	None
3 <sup>rd</sup> Party DLLs, Drivers, etc. and Version(s)	None
Additional file(s) loaded and version(s)	None
Record the disk image software version being used	Norton GHOST V:11.0
Record the filename of the build environment file signature (5.6.1.3) –	ESS_AutoMark_PreBuild_05272009.Hash.txt
Record the filename of the build environment disk image –	ESS_AutoMark_PreBuild_05272009.GHO
Verify (by signature) the build environment file signature (5.6.1.3)	Alastair Mayer, Sridevi Jakileti
<b>Loading Source Code (5.6.2)</b>	
Record the file signature of the source code (5.6.2.1)	see table of source code, above
Verify (by signature) that each file signature of the source code loaded matches as documented above (5.6.2.1)	Alastair Mayer, Sridevi Jakileti
Method of Build Witness	Trusted Build
Record the combined source code and pre-build environment file signature (5.6.2.2)	Prebuild_04142010_Automark_VAT.hash.txt
Record the combined source code and pre-build environment disk image (5.6.2.3)	Prebuild_04142010_Automark_VAT.GHO
Record the Final Build Version – Unique Identifier	VAT 1.3.2907
Certification Application Number (if applicable)	ESS0703
<b>Document during the Build Witness:</b>	
Date / Time Build Initiated	04/14/2010 08:30 am
Compiler and Version	See build tools and versions
Application Name	VAT
Application Version Order	1.3.2907
Obtain Names and Signatures of all persons present during build (record below)	Alastair Mayer, Sridevi Jakileti, Dave Herrera
Issue(s) and Resolution(s)	<p>1. AIMS is included in the image but was not built; only VAT was built.</p> <p>2. After the build, the Output folder was copied to the Staging folder. This step was not documented in the build instructions.</p> <p>3. The files “amcode.exe” and “w23code.dll” were copied from Install Creator to the Output folder. This step was not documented in the build instructions.</p> <p><a href="#">Resolved #151 &amp; 152 Unity 3.2.1.0 PCA and FCA Discrepancy Report</a></p>
<b>Document at Completion of the Build Witness:</b>	
Record the disk image of the final build (5.7.3)	PostBuild_04142010_AutoMark_VAT.GHO

Record file signature of the final build (5.6.3.1)	PostBuild_04142010_AutoMark_VAT.hash.txt
Record the type of unalterable storage media being used for installation disk(s) (i.e., CD) – (5.6.3.2)	CD
Record each piece of media that is part of the installation disk (each must have a unique identifier) (5.6.3.2, 5.7.5)	Install_04142010_AutoMark_VAT
Record the file signature of the installation disk(s). (5.6.3.3, 5.7.5) (include in below archive)	Install_04142010_AutoMark_VAT.hash.txt
Record the type of unalterable storage media being used for pre-build and post-build archive disk (i.e., CD) –	NAS2
Record each piece of media that is part of the pre-build archive disk (each must have a unique identifier) (5.6.2.4, 5.7.2, 5.7.3)	NAS2\ESS Unity 3.2.1.0\AutoMark_04142010_TB
Explanation of any significant differences observed	See Notes.

### 7.7.6 Witness of the Trusted Build of AutoMARK AIMS v. 1.3.257

Application/ Component	Version	Language	File Signature
AIMSESS DLL	1.0.1.0	C#	AIMS1.3.257_Source_10222009.hash.txt
AutomarkEncoder	1.0.105	C/C++	
MDB	1.3.257	VB	
SQL Server	1.3.054	SQL	

Document Prior to the Trusted Build:	
Vendor Name	ES&S
Vendor Consultant(s) (5.6)	Dave Herrera
Witness Name (5.6)	Sridevi Jakileti
Witness Title	Trusted Builder
Vendor Build Document(s) used and version(s)	AutoMARK AIMS Software Compilation Instructions .pdf Release date 9/17/2009
Equipment Used	DellOptiplexGX520
iBeta COTS used to clean the build environment disk (name and version) (5.6.1.1)	Restored the unity3.2.0.0 Post Cots image(ESS_AutoMark_PostCots_05222009.GHO)
iBeta COTS used to generate HASH file signatures (name and version)	Mares Hash Ver. 07.08.10.07.12
Construct the build environment (5.6.1.2)	
Verify (by signature) that the build environment is isolated and controlled by iBeta	Sridevi Jakileti
Witness attests to verifying that the source code being built is the source code provided by iBeta	Dave Herrera
Build Environment Operating System	Windows XP Professional Version 2002 Service Pack 2
Vendor CM Tool and version	None
Build tool(s) and version(s)	VAIO System Recovery DVD PCG-K23/PCG-K25/PCG-K27 Series Microsoft Embedded Visual C++ 4.0 Service Pack 4. Microsoft Visual Studio .NET 2003 Service Pack 2 Keil Software µVision2, C compiler Version 2.40 Texas Instruments Code Composer Studio. Version 2.0 Cosmic Compiler V 4.1H Borland C 4.02 Prog08sz Programmer for v 2.05 Atmel Flip v2.4.6 Atmel MCU ISP Software V1.0 Microsoft Access XP/2002

	InstallShield 10.5 Microsoft Windows CE With Platform Builder Version 5.0
3 <sup>rd</sup> Party Libraries and Version	ACCESSRT.MSI v2002,MSOHELP.exe 10.0.2609.0,Office1.cab v2002, OSP.MSI v2002,OSP1.cab v2002,FILESYSTEM\EXTRACT.exe v2002, FILESYSTEM\MLANG.DAT v2002,FILESYSTEM\MLANG.DLL 5.0.2919.6304,FILESYSTEM\MSXML.DLL 5.0.2919.6303, FILESYSTEM\T2EMBED.DLL 0.2.0.69,FILESYSTEM\WINDOWS\HELP\OSP.HLP v2002,IE5\EN\ACTSETUP.cab v2002,IE5\EN\ADVAUTH.cab v2002, IE5\EN\VAOLSUPP.cab v2002,IE5\EN\AXA.cab v2002,IE5\EN\AXA2.cab v2002,IE5\EN\AXA3.cab v2002,IE5\EN\BRANDING.cab v2002, IE5\EN\DCOM95.exe 4.71.1015.0,IE5\EN\DXDDEX.cab v2002,IE5\EN\DXMINI.cab v2002,IE5\EN\FONTCORE.cab v2002, IE5\EN\FONTSUP.cab v2002,IE5\EN\FPESETUP.cab v2002,IE5\EN\GSETUP95.cab v2002,IE5\EN\GSETUPNT.cab v2002, IE5\EN\HELPCONT.cab v2002,IE5\EN\HHUPD.cab v2002,IE5\EN\ICW.cab v2002,IE5\EN\ICWCON.cab v2002, IE5\EN\IE4MFC40.cab v2002,IE5\EN\IE4SHL95.cab v2002,IE5\EN\IE4SHLNT.cab v2002,IE5\EN\IE5COMP.exe 5.0.2919.6307 IE5\EN\IE5SETUP.exe 5.0.2919.6307,IE5\EN\IECIF.cab v2002,IE5\EN\IEDATA.cab v2002,IE5\EN\IEDATAJA.cab v2002, IE5\EN\IELPKAD.cab v2002,IE5\EN\IELPKAR.cab v2002,IE5\EN\IELPKIW.cab v2002,IE5\EN\IELPKJA.cab v2002, IE5\EN\IELPKKO.cab v2002,IE5\EN\IELPKPE.cab v2002,IE5\EN\IELPKTH.cab v2002,IE5\EN\IELPKVI.cab v2002, IE5\EN\IELPKZHC.cab v2002,IE5\EN\IELPKZHT.cab v2002,IE5\EN\IENT_S1.cab v2002,IE5\EN\IENT_S2.cab v2002, IE5\EN\IENT_S3.cab v2002,IE5\EN\IENT_S4.cab v2002,IE5\EN\IENT_S5.cab v2002,IE5\EN\IESETUP.INI v2002, IE5\EN\IE_EXTRA.cab v2002,IE5\EN\IE_S1.cab v2002,IE5\EN\IE_S2.cab v2002,IE5\EN\IE_S3.cab v2002, IE5\EN\IE_S4.cab v2002,IE5\EN\JAIME.cab v2002,IE5\EN\KOAIME.cab v2002,IE5\EN\MAILNEWS.cab v2002, IE5\EN\MDAC_1E5.cab v2002,IE5\EN\MOBILE95.cab v2002,IE5\EN\MOBILENT.cab v2002,IE5\EN\MPCDCS.cab v2002, IE5\EN\MPPLAYER2.cab v2002,IE5\EN\MSN_AUTH.cab v2002,IE5\EN\NM30.cab v2002,IE5\EN\OAINST.exe 4.71.1015.0 IE5\EN\SCAIME.cab v2002,IE5\EN\SETUPNT.cab v2002,IE5\EN\SETUPW95.cab v2002,IE5\EN\SWDIR.cab v2002, IE5\EN\SWFLASH.cab v2002,IE5\EN\TCAIME.cab v2002,IE5\EN\TS95.cab v2002,IE5\EN\TSNT.cab v2002, IE5\EN\USP10.cab v2002,IE5\EN\VBSRIPT.cab v2002,IE5\EN\VGX.cab v2002,IE5\EN\VMX86_01.cab v2002, IE5\EN\VMX86_02.cab v2002,IE5\EN\VRML2C.exe 4.71.1015.0,IE5\EN\WAB.cab v2002,IE5\EN\WEBFLDRS.cab v2002, IE5\EN\WPIE5X86.cab v2002,chs.syn 6.1.0.0,chsrom.DLL 6.1.0.0,eci.DLL 6.1.0.0,enu.syn 6.1.0.0 esm.syn 6.1.0.0,jpn.syn 6.1.0.0,jpnrom.DLL 6.1.0.0,kor.syn 6.1.0.0,korrom.DLL 6.1.0.0,ARIALUNI.TTF,BATANG.TTF MSMINCHO.TTF,PMINGLIU.TTF,sqlxml.MSI c3.0,xblkId3.DLL 3.30.3457.0,Helper.exe,SqlRun.cab,,SqlRun01.MSI 1033dotnetfx.exe 1.1.4322.573,1033,dotnetfxSp1.exe 1.0.0.0,dotnetfxSp1.exe 1.0.871.2738 chs.syn v6.1.0.0,chsrom.DLL v6.1.0.0,eci.DLL v6.1.0.0,enu.syn v6.1.0.0,esm.syn v6.1.0.0,jpn.syn v6.1.0.0,jpnrom.DLL v6.1.0.0,kor.syn v6.1.0.0,korrom.DLL v6.1.0.0,chs.syn v6.1.0.0,chsrom.DLL v6.1.0.0,eci.DLL v6.1.0.0,enu.syn v6.1.0.0,esm.syn v6.1.0.0,FTD2XX.DLL v6.1.0.0,ftd2xx.inf v6.1.0.0,ftdi_d2xx.DLL v6.1.0.0,jpn.syn v6.1.0.0,jpnrom.DLL v6.1.0.0,kor.syn v6.1.0.0,korrom.DLL

	v6.1.0.0,Microsoft.WindowsCE.Forms.DLL v1.0.2268.0, MSCORLIB.DLL v1.0.2268.0,regflush.exe System.DATa.Common.DLL 1.0.2268.0,ICSharpCode.SharpZipLib.DLL 0.85.1.271,New Text Document.txt 0.85.1.271,SharpZipLib_0855_Bin[1].zip 0.85.1.271,cabwiz.ddf,Cabwiz.exe 3.1.0.9386,CFResGen.exe 1.0.4128.0, Makecab.exe, unzip.exe 5.52, WinCEPB50-060430-2006M04-Armv4I.msi V5.0,WinCEPB50- 060831-2006M08-Armv4I.msi V5.0,WinCEPB50-060228-2006M02- Armv4I.msi V5.0,WinCEPB50-060131-2006M01-Armv4I.msi V5.0,WinCEPB50-060731-2006M07-Armv4I.msi V5.0,WinCEPB50- 060630-2006M06-Armv4I.msi V5.0,WinCEPB50-060331-2006M03- Armv4I.msi V5.0, WinCEPB50-060531-2006M05-Armv4I.msi V5.0,WinCEPB50- 041231-Product-Update-Rollup-Armv4I.msi V5.0,WinCEPB50- 051231-Product-Update-Rollup-Armv4I.msi V5.0,autoit-v3-setup.exe 3.3.0.0, ADS_XSCALE_4_2_SDK.msi, DATA.TAG v2.4.6,data1.cab v2.4.6, lang.dat v2.4.6,layout.bin v2.4.6, os.dat v2.4.6,setup.bmp v2.4.6, SETUP.EXE v2.4.6,SETUP.INI v2.4.6, setup.ins v2.4.6,setup.lid v2.4.6, _INST32I.EX_ v2.4.6,_ISDEL.EXE v2.4.6, _setup.dll v2.4.6,_sys1.cab v2.4.6, _user1.cab v2.4.6,evc4sp4.exe v4 PL2303.CAT,SER2PL.INF,SER2PL.SYS DISK.INI v7.09,c51util.dll v7.09,TX51TNY.LIB v7.09,CONF_TNY.A51 v7.09,DBG_TINY.DSW v7.09, GENRTX.BAT v7.09,READ.ME2 v7.09, RIGHT.A51 v7.09,RTX51TNY.A51 v7.09, VERS.A51 v7.09,
3 <sup>rd</sup> Party Source Code (COTS) and Version	None
3 <sup>rd</sup> Party DLLs, Drivers, etc. and Version(s)	None
Additional file(s) loaded and version(s)	None
Record the disk image software version being used	Norton GHOST V:11.0
Record the filename of the build environment file signature (5.6.1.3) –	ESS_AutoMark_PostCots_05222009.hash.txt(Hash from 3.2.0.0 Build)
Record the filename of the build environment disk image –	Restored the Image from the previous build from 3.2.0.0(ESS_AutoMark_PostCots_05222009.GHO)
Verify (by signature) the build environment file signature (5.6.1.3)	Sridevi Jakileti
<b>Loading Source Code (5.6.2)</b>	
Record the file signature of the source code (5.6.2.1)	see table of source code, above
Verify (by signature) that each file signature of the source code loaded matches as documented above (5.6.2.1)	Sridevi Jakileti
Method of Build Witness	TrustedBuild
Record the combined source code and pre-build environment file signature (5.6.2.2)	Unity3.2.1.0_AIMS1.3.257_PrepBuild_10222009.hash.txt
Record the combined source code and pre-build environment disk image (5.6.2.3)	AIMS_PrepBuild_10222009.gho
Record the Final Build Version – Unique Identifier	AIMS1.3.257
Certification Application Number (if applicable)	ESS0703
<b>Document during the Build Witness:</b>	
Date / Time Build Initiated	10/22/2009 11.30am
Compiler and Version	See build tools and versions

Application Name	AIMS
Application Version Order	1.3.257
Obtain Names and Signatures of all persons present during build (record below)	Dave Herrera, Sridevi Jakileti
Issue(s) and Resolution(s)	No Issues
<b>Document at Completion of the Build Witness:</b>	
Record the disk image of the final build (5.7.3)	AIMS_PostBuild_10222009.GHO
Record file signature of the final build (5.6.3.1)	Unity3.2.1.0_AIMS1.3.257_PostBuild_10222009.hash.txt
Record the type of unalterable storage media being used for installation disk(s) (i.e., CD) – (5.6.3.2)	CD
Record each piece of media that is part of the installation disk (each must have a unique identifier) (5.6.3.2, 5.7.5)	AIMS1.3.257 Trusted Build 10222009
Record the file signature of the installation disk(s). (5.6.3.3, 5.7.5) (include in below archive)	AIMS 1.3.257_Installs_10222009.hash.txt
Record the type of unalterable storage media being used for pre-build and post-build archive disk (i.e., CD) –	NAS2
Record each piece of media that is part of the pre-build archive disk (each must have a unique identifier) (5.6.2.4, 5.7.2, 5.7.3)	Nas2\ESS Unity 3.2.1.0\Unity3.2.1.0_TrustedBuild_AIMS_10222009
Explanation of any significant differences observed	None

Notes:

- There is no source code difference in version 1.3.157 and 1.3.257, but there is a difference in Build package “AIMS ESS Installation.ism” is different, as per AIMS 3010 System Change Notes updated the AIMS ESS Installation.ism to allow AIMS to run in a multi-user environment.

### 7.7.7 **Witness of the Trusted Build of DS200TOS v.1.0.2.0**

Application/ Component	Version	Language	File Signature
BLFS_1.0.1.0_BuildPkg.iso	1.0.2.0	Scripts and makefiles	DS200 BLFS 1.0.2.0 Build Package_TB_07192010.hash.txt

<b>Document Prior to the Trusted Build:</b>	
Vendor Name	ES&S 3.2.1.0
Vendor Consultant(s) (5.6)	Dave Herrera
Witness Name (5.6)	Sridevi Jakileti
Witness Title	Trusted Builder
Vendor Build Document(s) used and version(s)	DS200 Target Operating System(TOS) version1.0.2.0
Equipment Used	Dell #E085 Slot1
ibeta COTS used to clean the build environment disk (name and version) (5.6.1.1)	Active KillDisk for DOS V:4.1 Build 2380
iBeta COTS used to generate HASH file signatures (name and version)	Mares Hash Ver. 07.08.10.07.12
<b>Construct the build environment (5.6.1.2)</b>	
Verify (by signature) that the build environment is isolated and controlled by iBeta	Sridevi Jakileti
Witness attests to verifying that the source code being built is the source code provided by iBeta	Sridevi Jakileti
Vendor CM Tool and version	Concurrent Versions System (CVS) 1.11.22
Build Environment Operating System	Linux operating system

Build tool(s) and version(s)	Linux From Scratch 6.25
3 <sup>rd</sup> Party Libraries and Version	LFS Live CD X86-6.2.5
3 <sup>rd</sup> Party Source Code (COTS) and Version	Please see build procedure DS200 Target Operating System (TOS) Version 1.0.2.0, Document Version 1.0, June 25, 2010
3 <sup>rd</sup> Party DLLs, Drivers, etc. and Version(s)	bdftopcf-1.0.2.tar.bz2 ,bigreqsproto-1.1.0.tar.bz2 , BLFS-ca-bundle-3.12.5.tar.bz2 ,cairo-1.8.10.tar.gz , compositeproto-0.4.1.tar.bz2 ,damageproto-1.2.0.tar.bz2 , dmxproto-2.3.tar.bz2 ,dri2proto-2.2.tar.bz2 ,encodings-1.0.3.tar.bz2 , expat-2.0.1.tar.gz ,fixesproto-4.1.1.tar.bz2 ,font-adobe-100dpi-1.0.1.tar.bz2 , font-adobe-75dpi-1.0.1.tar.bz2 ,font-adobe-utopia-100dpi-1.0.2.tar.bz2 ,font- adobe-utopia-75dpi-1.0.2.tar.bz2 , font-adobe-utopia-type1-1.0.2.tar.bz2 ,font-alias-1.0.2.tar.bz2 , font-arabic-misc-1.0.1.tar.bz2 ,font-bh-100dpi-1.0.1.tar.bz2 , font-bh-75dpi-1.0.1.tar.bz2 ,font-bh-lucidatypewriter-100dpi-1.0.1.tar.bz2 ,font- bh-lucidatypewriter-75dpi-1.0.1.tar.bz2 , font-bh-ttf-1.0.1.tar.bz2 ,font-bh-type1-1.0.1.tar.bz2 , font-bitstream-100dpi-1.0.1.tar.bz2 ,font-bitstream-75dpi-1.0.1.tar.bz2 ,font- bitstream-type1-1.0.1.tar.bz2 , fontconfig-2.8.0.tar.gz ,font-cronyx-cyrillic-1.0.1.tar.bz2 , font-cursor-misc-1.0.1.tar.bz2 ,font-daewoo-misc-1.0.1.tar.bz2 , font-dec-misc-1.0.1.tar.bz2 ,font-ibm-type1-1.0.1.tar.bz2 , font-isas-misc-1.0.1.tar.bz2 ,font-jis-misc-1.0.1.tar.bz2 , font-micro-misc-1.0.1.tar.bz2 ,font-misc-cyrillic-1.0.1.tar.bz2 , font-misc-ethiopic-1.0.1.tar.bz2 ,font-misc-meltho-1.0.1.tar.bz2 , font-misc-misc-1.1.0.tar.bz2 ,font-mutt-misc-1.0.1.tar.bz2 , font-schumacher-misc-1.1.0.tar.bz2 ,font-screen-cyrillic-1.0.2.tar.bz2 ,font- sony-misc-1.0.1.tar.bz2 ,fontsproto-2.1.0.tar.bz2 , font-sun-misc-1.0.1.tar.bz2 ,font-util-1.1.1.tar.bz2 , font-winitzki-cyrillic-1.0.1.tar.bz2 ,font-xfree86-type1-1.0.2.tar.bz2 , freetype-2.3.12.tar.bz2 ,glproto-1.4.11.tar.bz2 , iceauth-1.0.3.tar.bz2 ,inputproto-2.0.tar.bz2 ,intltool-0.40.6.tar.bz2 , kbproto-1.0.4.tar.bz2 ,libdmx-1.1.0.tar.bz2 ,libdrm-2.4.14.tar.bz2 , libfontenc-1.0.5.tar.bz2 ,libFS-1.0.2.tar.bz2 ,libICE-1.0.6.tar.bz2 , libpciaccess-0.11.0.tar.bz2 ,libpng-1.2.42.tar.bz2 , libpthread-stubs-0.1.tar.bz2 ,libSM-1.1.1.tar.bz2 , libX11-1.3.3.tar.bz2 ,libXau-1.0.5.tar.bz2 ,libXaw-1.0.7.tar.bz2 , libXcomposite-0.4.1.tar.bz2 ,libXcursor-1.1.10.tar.bz2 , libXdamage-1.1.2.tar.bz2 ,libXdmcp-1.0.3.tar.bz2 , libXext-1.1.1.tar.bz2 ,libXfixes-4.0.4.tar.bz2 ,libXfont-1.4.1.tar.bz2 , libXft-2.1.14.tar.bz2 ,libXi-1.3.tar.bz2 ,libXinerama-1.1.tar.bz2 , libXkbfile-1.0.6.tar.bz2 ,libXmu-1.0.5.tar.bz2 , libXpm-3.5.8.tar.bz2 ,libXrandr-1.3.0.tar.bz2 , libXrender-0.9.5.tar.bz2 ,libXres-1.0.4.tar.bz2 , libXScrnSaver-1.2.0.tar.bz2 ,libXt-1.0.7.tar.bz2 , libXtst-1.1.0.tar.bz2 ,libXv-1.0.5.tar.bz2 ,libXvMC-1.0.5.tar.bz2 , libXxf86dga-1.1.1.tar.bz2 ,libXxf86vm-1.1.0.tar.bz2 , makedepend-1.0.2.tar.bz2 ,mkfontdir-1.0.5.tar.bz2 , mkfontscale-1.0.7.tar.bz2 ,openssl-0.9.8n.tar.gz , openssl-0.9.8n-fix_manpages-1.patch ,pixman-0.15.20.tar.gz , pkg-config-0.22.tar.gz ,randproto-1.3.1.tar.bz2 , recordproto-1.14.tar.bz2 ,renderproto-0.11.tar.bz2 , resourceproto-1.1.0.tar.bz2 ,scrn saverproto-1.2.0.tar.bz2 , sessreg-1.0.5.tar.bz2 ,setxkbmap-1.1.0.tar.bz2 , smproxy-1.0.3.tar.bz2 ,twm-1.0.4.tar.bz2 ,util-macros-1.5.0.tar.bz2 , videoproto-2.3.0.tar.bz2 ,x11perf-1.5.1.tar.bz2 , xauth-1.0.4.tar.bz2 ,xbacklight-1.1.1.tar.bz2 ,xbitmaps-1.1.0.tar.bz2 , xclock-1.0.4.tar.bz2 ,xcmiscproto-1.2.0.tar.bz2 ,xcmsdb-1.0.2.tar.bz2 , xcursorgen-1.0.3.tar.bz2 ,xcursor-themes-1.0.2.tar.bz2 ,xdpyinfo-1.1.0.tar.bz2 , xdiinfo-1.0.3.tar.bz2 ,xev-1.0.4.tar.bz2 , xextproto-7.1.1.tar.bz2 ,xf86bigfontproto-1.2.0.tar.bz2 ,xf86dgaproto- 2.1.tar.bz2 ,xf86driproto-2.1.0.tar.bz2 , xf86-input-keyboard-1.4.0.tar.bz2 ,xf86-input-mouse-1.5.0.tar.bz2 , xf86-video-vesa-2.3.0.tar.bz2 ,xf86vidmodeproto-2.3.tar.bz2 , xgamma-1.0.3.tar.bz2 ,xhost-1.0.3.tar.bz2 ,xineramaproto-1.2.tar.bz2 ,xinit- 1.2.0.tar.bz2 ,xinput-1.5.0.tar.bz2 ,xkbcproto-1.1.1.tar.bz2 , xkbevd-1.1.0.tar.bz2 ,xkbutils-1.0.2.tar.bz2 ,xkeyboard-config-1.7.tar.bz2 ,xkill- 1.0.2.tar.bz2 ,xlsatoms-1.0.2.tar.bz2 , xlsclients-1.0.2.tar.bz2 ,XML-Parser-2.36.tar.gz , xmodmap-1.0.4.tar.bz2 ,xorg-server-1.7.1.tar.bz2 , xpr-1.0.3.tar.bz2 ,xprop-1.1.0.tar.bz2 , xproto-7.0.16.tar.bz2 ,xrandr-1.3.2.tar.bz2 ,

	xrdb-1.0.6.tar.bz2 ,xrefresh-1.0.3.tar.bz2 ,xset-1.1.0.tar.bz2 , xsetroot-1.0.3.tar.bz2 ,xterm-254.tgz ,xtrans-1.2.5.tar.bz2 , xvinfo-1.1.0.tar.bz2 ,xwd-1.0.3.tar.bz2 ,xwininfo-1.0.5.tar.bz2 , xwud-1.0.2.tar.bz2 ,aumix-2.8.tar.bz2 ,beecrypt-4.1.2.tar.gz ,blfs-bootscripts- 20060910.tar.bz2 ,BLFS-ca-bundle-3.12.5.tar.bz2 ,boost_1_34_1.tar.bz2 , busybox-1.2.1.tar.bz2 ,cryptome-2.0-rhel30.tar.gz ,ctags-5.6.tar.gz ,cvs- 1.11.22.tar.bz2 ,cvs-1.11.22-zlib-1.patch ,dosfstools-2.11.src.tar.gz , e2fsprogs-1.38.tar.bz2 ,expat-2.0.1.tar.gz ,gpm-1.20.1.tar.bz2 ,gpm-1.20.1- segfault-1.patch ,gpm-1.20.1-silent-1.patch ,ibusb-0.1.12.tar.gz ,linux-libc- headers-2.6.12.0.tar.bz2 ,openssh-4.5p1.tar.gz ,openssl-0.9.8n.tar.gz , openssl-0.9.8n-fix_manpages-1.patch ,pkg-config-0.22.tar.gz ,unzip552.tar.gz , usbutils-0.72.tar.gz ,zip232.tar.gz ,apache-ant-1.7.0-bin.zip ,atk- 1.11.4.tar.bz2 ,bootsplash-3.2.tar.bz2 ,bootsplash-3.2_makefile.patch ,glib- 4.1.4.tar.bz2 ,glib-2.10.3.tar.bz2 ,glibmm-2.12.10.tar.bz2 ,gtk+-2.8.20.tar.bz2 , gtkmm-2.8.12.tar.bz2 ,jdk-6u3-linux-i586.bin ,jpegsrc.v6b.tar.gz ,jre-6u3-linux- i586.bin ,lcms-1.14.tar.gz ,lcms-1.14-gcc343-1.patch ,pango-1.12.3.tar.bz2 , tiff-3.8.2.tar.gz ,bootplash-3.1.6-2.6.15.diff ,linux-2.6.16.27.tar.bz2 ,linux- 2.6.16.27-utf8_input-1.patch ,udev-096.tar.bz2
Additional file(s) loaded and version(s)	LFS1.sh,BLFS1.sh,BLFS2.sh,BLFS3.sh, TOS1.sh,VersionNumbers.txt, BLFS_1.0.2.0_BuildPkg.
Record the disk image software version being used	Norton GHOST V:11.0
Record the filename of the build environment file signature (5.6.1.3) –	DS200TOS_PostCots_07192009.hashl
Record the filename of the build environment disk image –	DS200TOS_PostCots_07192009.GHO
Verify (by signature) the build environment file signature (5.6.1.3)	Sridevi Jakileti
<b>Loading Source Code (5.6.2)</b>	
Record the file signature of the source code (5.6.2.1)	see table of source code, above
Verify (by signature) that each file signature of the source code loaded matches as documented above (5.6.2.1)	Sridevi Jakileti
Method of Build Witness	Trusted Build
Record the combined source code and pre-build environment file signature (5.6.2.2)	DS200TOS1.0.2.0_PreBuild_07202010.hashl
Record the combined source code and pre-build environment disk image (5.6.2.3)	DS200TOS_PreBuild_07202009.GHO
Record the Final Build Version – Unique Identifier	DS200TOS 1.0.1.0
Certification Application Number (if applicable)	ESS0703
<b>Document during the Build Witness:</b>	
Date / Time Build Initiated	7/20/2010 8.45am
Compiler and Version	GCC-4.0.3 (GNU Compiler Collection). This compiler is part of the LFS (Linux From Scratch) 6.2-5 Live CD
Application Name	CfCard_ds200_n1.0.2.0 (DS200 Target operating system)
Application Version Order	None
Obtain Names and Signatures of all persons present during build (record below)	SJakileti, Dave Herrera
Issue(s) and Resolution(s)	No Issues
<b>Document at Completion of the Build Witness:</b>	
Record the disk image of the final build (5.7.3)	DS200TOS_PostBuild_07192009.GHO
Record file signature of the final build (5.6.3.1)	DS200TOS1.0.2.0_PostBuild_07202010.hashl
Record the type of unalterable storage media being used for installation disk(s) (i.e., CD) – (5.6.3.2)	NAS2
Record each piece of media that is part of the installation disk (each must have a unique identifier) (5.6.3.2, 5.7.5)	NAS2

Record the file signature of the installation disk(s). (5.6.3.3, 5.7.5) (include in below archive)	ESS_DS200TOS_TBInstall07202009.hash.txt
Record the type of unalterable storage media being used for pre-build and post-build archive disk (i.e., CD) –	NAS2 drive
Record each piece of media that is part of the pre-build archive disk (each must have a unique identifier) (5.6.2.4, 5.7.2, 5.7.3)	NAS2 drive
Explanation of any significant differences observed	No differences

### 7.7.8 ES&S Validation Tools

As identified in Section 5.8 and 5.9 of the *US Election Assistance Commission Test and Certification Program Manual* delivery of the System Identification Tools to the EAC is the responsibility of ES&S. Review of the System Identification Tools is the responsibility of the EAC. iBeta reviewed the installation documentation to the requirements of v.2: 2.6.4 ([See Appendix C: PCA TDP Document Review](#)).

## **7.8 Appendix H: Amended Test Plan**

The [ES&S Unity 3.2.1.0 VSTL Certification Test Plan v.5.0](#), the [Approval Letter - Test Plan Ver. 5.0 and Approval of Reuse of SysTest Prior Testing for ES&S Unity 3.2.1.0](#) are found on the EAC website.

This test plan was amended during test execution. Version 6.0 of the amended test plan is attached.

## **7.9 Appendix I: State Test Reports**

There were no state test reports issued concurrent to the certification testing of Unity 3.2.1.0.

## **7.10 Appendix J Unity 3.2.1.0 Implementation Statement**

A copy of the Unity 3.2.1.0 implementation statement shall be attached to the certification report when testing is completed.

## 7.11 Appendix K Unity 3.2.1.0 List of Changes Submitted in Unity 3.2.1.0

The change orders (CO) listed below were submitted by ES&S as changes to the certified Unity 3.2.0.0 system. The CO's displayed below are tested and accepted for use with the Unity 3.2.1.0 voting system.

- Change ID: Vendor designated identification of the change
- System : The system or system component that the change applies to
- Description: Description of the change made to the system and typically the reason why (i.e. discrepancy)
- Mandatory: Is the change designated to be a mandatory change (i.e. fix a test or field issue)?
- Deminimis: Is the change agreed to by the vendor, lab, and EAC to be deminimis?
- Tested: Indicates whether the change is included in the tested configuration or not and may include added information about the type of testing
- Note: Indicate relevant information about the change that helps users with applicability or source references

Change ID	System	Description	Mandatory	Deminimis	Tested	Note
<b>SW/FW</b>						
BUG17375	DS200	Fix source code discrepancies per VSTL review.	Mandatory Build v. 1.4.3.7	No	Yes - SCR Func	Source code review and DS200 Functional TC
BUG17664	DS200	Fix source code discrepancies per VSTL review.	Mandatory Build v. 1.4.3.7	No	Yes - SCR Func	Source code review and DS200 Functional TC
BUG15827	DS200	Resolved an issue where the scanner failed to divert overvoted write-in ballots when the "Divert Write-ins" option was selected	Mandatory Build v. 1.4.3.7	No	Yes - Func	
BUG16775	DS200	Resolved an issue that caused L&A test decks to yield incorrect vote totals- (See /Field Issue #1)	Mandatory Build v. 1.4.3.7	No	Yes - Func	
BUG16782	DS200	Resolved an issue that caused L&A test decks to yield incorrect vote totals- (See /Field Issue #1)	Mandatory Build v. 1.4.3.7	No	Yes - Func	
BUG17666	DS200	Added the protected count to the status report that prints automatically when a DS200 is re-opened for voting.	Mandatory Build v. 1.4.3.7	No	Yes - Func	
BUG18361	DS200	Updated the HAL (Hardware Abstraction Layer) client to resolve instances where pointers to statically-initialized data were being returned.	Mandatory Build v. 1.4.3.7	No	Yes - SCR Func	
BUG18687	DS200	Resolved an issue that erroneously prevented contest and candidate names from appearing on zero reports.	Mandatory Build v. 1.4.3.7	No	Yes - Func	This was found on a build not submitted to iBeta.
BUG18770	DS200	Fix source code discrepancies per VSTL review.	Mandatory Build v. 1.4.3.7	No	Yes - SCR Func	Source code review and DS200 Functional TC
BUG19664	DS200	Updated the system to ensure all error messages that can be logged are written to the internal audit log.	Mandatory Build v. 1.4.3.7	No	Yes - SCR Func	
BUG19853	DS200	Resolved a condition where the system continued to accept ballots after an Audit Log full condition was detected.	Mandatory Build v. 1.4.3.7	No	Yes - SCR Func	
BUG13633	ERM	Resolved an issue that caused ERM to error out during database creation when the System Type in HPM is set to Central Count	Mandatory Build v.7.5.7.0	No	Yes - SCR Func	Discrepancy 20 (Issue 104 transferred from Unity 3.2.0.0)
BUG15585	ERM	Corrected an issue in which ERM was populating removing leading zeroes from the 'Candidate altNumber' attribute in the state results transfer file rather than populating the attribute with the full, 19-character value required by the State of Minnesota.	Mandatory Build v.7.5.7.0	No	No	Minnesota specific, testing deferred to Minnesota state certification
BUG16384	ERM	Resolved an issue with overvote reporting	Mandatory	No	Yes -	

<b>Change ID</b>	<b>System</b>	<b>Description</b>	<b>Mandatory</b>	<b>Demini mis</b>	<b>Tested</b>	<b>Note</b>
		where the overvote total reported matched the number of ballots reporting the overvote rather than the number of votes lost due to an overvote.	Build v.7.5.7.0		SCR Func	
ENH14725	DS200	Remove Image Drive icon from DS200 if images are not being saved	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH14726	DS200	Extend the time that "Thank you for voting" displays	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH14728	DS200	Provide clear indication that modem transfer was successful	Mandatory Build v. 1.4.3.7	No	Yes - SCR	Source code review to the VVSG Vol. 1 Sect. 5.2 - 5.2.7 & Vol. 2 Sect. 5.4 - 5.4.2. (Modem functionality is not supported in Unity 3.2.0.0 Rev 1. iBeta confirmed the DS200 modem was removed from the system configuration submitted for testing)
ENH14729	DS200	Allow multiple zeros tapes to be printed before the first ballot is cast	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH14730	DS200	Change continuous alert beeping to just two beeps	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH14731	DS200	Issue audible alarm when ballot is accepted	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH14732	DS200	Repeat machine ID and poll number at end of results tape	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH14745	DS200	Provide override for overvote or blank ballot rejection	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH15009	DS200	Implement Counterfeit Ballot Sensor	Mandatory Build v. 1.4.3.7	No	Yes - Func	Detection of counterfeit ballots functionality failed testing and was withdrawn. This functionality is not required by the VVSG. **Disabled counterfeit detection functionality in ENH19328
ENH15287	DS200	Add Early Voting Ballot Styles per Precinct Report	Mandatory Build v. 1.4.3.7	No	Yes	
ENH15288	DS200	Increase Font Size of Thank you for Voting message	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH15418	DS200	Small white dots "hickeys" causing read problems	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH15890	DS200	Implement new scanner board firmware	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH15891	DS200	Implement new administration functionality to calibrate counterfeit sensor	Mandatory Build v. 1.4.3.7	No	Yes - Func	**Disabled counterfeit sensor functionality in ENH19328
ENH15892	DS200	Update scanner client to work with new	Mandatory	No	Yes -	

<b>Change ID</b>	<b>System</b>	<b>Description</b>	<b>Mandatory</b>	<b>Demini mis</b>	<b>Tested</b>	<b>Note</b>
		scanner board firmware	Build v. 1.4.3.7		Func	
ENH16085	DS200	Install New Icons on Welcome Screen	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH16120	DS200	Updated the overvote warning screen	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH16211	DS200	Print Machine ID & Poll Number in Audit Log and after report cancellations	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH16231	DS200	Enhanced audit logging to log all user actions in the Administration menu and attempts to access the Administration menu.	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH16291	DS200	DS200: Additional language translations for the overvote screen	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH16336	DS200	DS200: Update language translations for the overvote screen	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH16382	DS200	Expand Election Day capacity to 18 precincts	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH17266	DS200	Updated scanner board version.	Mandatory Build v2.20.0.0	No	Yes - Func	
ENH17268	DS200	Promoted DS200 version implemented in Florida for use in Unity 3200r1.	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH17538	DS200	Added a protected count to the DS200 firmware. The protected count resides on the compact flash card in the ES&S firmware partition. It will increment with every sheet accepted and dropped into the ballot box. The counter must appear in printed reports.	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH18150	DS200	Test build supplied to VSTL to confirm that updating DS200 system firmware does not delete the protected counter	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH18296	DS200	Enhanced the DS200 to reset the pointer used to free allocated memory to a "NULL" state after memory is freed.	Mandatory Build v. 1.4.3.7	No	Yes – SCR Func	
ENH18555	DS200	Added event log entries for a condition where the DS200 is shut down while awaiting a voter response to a "hold ballot" event ('query voter,' automatic acceptance or automatic rejection).	Mandatory Build v. 1.4.3.7	No	Yes – SCR Func	
ENH18562	DS200	Added functionality to gracefully shut the system down in the event menus terminate unexpectedly.	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH18681	DS200	Disabled the screen hibernation between voters.	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH18807	DS200	Added a screen message that displays upon recovering from a condition in which the DS200 is shut down while awaiting a voter response to a "hold ballot" event ('query voter,' automatic acceptance or automatic rejection).	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH18851	DS200	Updated the DS200 operating system to resolve unexpected system freezes.	Mandatory Build	No	Yes - SCR	

Change ID	System	Description	Mandatory	De minimis	Tested	Note
			v. 1.4.3.7		Func	
ENH18865	DS200	Added functionality to check the CRC of the system log sections of the PCB file on the removable USB Flash drive when the drive is inserted into the machine and initialized.	Mandatory Build v. 1.4.3.7	No	Yes - SCR Func	
ENH19168	DS200	Add audit log entry for each time the DS200 casts a ballot.	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH19169	DS200	Add audit log entry for each time the DS200 powers up.	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH19170	DS200	Add audit log entry for each time the DS200 powers off.	Mandatory Build v. 1.4.3.7	No	Yes - Func	
ENH19323	DS200	Disable counterfeit detection and sensor functionality (ENH15009 and 15891)	Mandatory Build v. 1.4.3.7	No	Yes - Func & SCR	DS200 Functional TC and Source Code Review
ENH19663	DS200	Added a modem status message to the audit log and initial configuration report. The initial configuration report now catalogs the presence or absence of a modem.	Mandatory Build v. 1.4.3.7	No	Yes - Func & SCR	
ENH19936	DS200	Resolved a condition that allowed an operator to access DS200 administrative menus after a firmware update failure.	Mandatory Build v. 1.4.3.7	No	Yes - Func & SCR	
ENH17702	HPM	Added a warning message prior to the creation of final database files if the created election exceeds 18 precincts for the M100 and DS200 equipment types.	Mandatory Build v. 5.7.3.0	No	Yes - Func & SCR	Discrepancy # 67
ENH17725	HPM	Enhanced error messages related to programming PC Cards for the Model 100. Improved messaging provides additional guidance for resolving issues.	Mandatory Build v. 5.7.3.0	No	Yes - Func & SCR	Discrepancy # 107

Change ID	System	Description	Mandatory	De Minimis	Tested	Note
<b>Hardware</b>						
000315	DS200	Ballot Box Carrying Case - Glue for foam	Optional	Yes	Yes	This change did not require any testing however; the carrying case with ECO 000315 was delivered by ES&S as part of the configuration under test.
000337	DS200	Ballot Bin status change Rev 1.3	Optional	Yes	No	Document change
000332	DS200	DS200 Ballot Box new lock	Optional	No	Yes - EMC	
000339	DS200	DS200 Ballot Box carry case-washer & rivet to hold foam	Optional	No	Yes - EMC	This change did not require any testing however; the carrying case with ECOs 000359 & 000332 was delivered by ES&S as part of the configuration under test.
000342	DS200	DS200 Ballot Box BOM status change	Optional	Yes	No	Document change
000359	DS200	DS200 Adding metal bottom edge (BOM & engineering status change)	Optional	No	Yes - EMC	
000366	DS200	Ballot Box - Retrofit Stock	Optional	Yes	No	Document change only
000375	DS200	DS200 Carrying Case Drawings	Optional	Yes	No	Document change only

Change ID	System	Description	Mandatory	De Minimis	Tested	Note
000423	DS200	Ballot Box -Shipping	Optional	Yes	No	Document change/spacer packaging
000466	DS200	DS200 Ballot Box -Caster Bolt (2nd source)	Optional	Yes	No	
836	Steel Ballot box	Steel Ballot Box – Retractable Security Pin	Optional	Yes	No	
837	USB	COTS Thumb Drive Housing	Optional	Yes	Yes - Func	The Delkin 4gb and 8gb cover was tested with ECO 838 in "DS200 Functional & Regression TC"
838	SUB	COTS Thumb drive controller	Optional	No	Yes - Func	The Delkin 4gb and 8gb have been updated with firmware residing on the controller chip, requiring Functional Testing.
839	DS200	DS200 -label for compact flash	Optional	Yes	No	Document change
841	DS200	DS200 EOL Sensor, Power Switch & Capacitor	Optional	No	Yes - EMC	
843	Steel Ballot box	Steel ballot box -Diverter cable	Optional	No	Yes - EMC	
844	DS200	DS200 EOL parts	Optional	No	Yes - EMC	
845	Steel Ballot box	Steel Ballot Box -caster change	Optional	Yes	No	
846	DS200	DS200 document part number	Optional	Yes	No	This change did not require any testing however; this was delivered by ES&S as part of the configuration under test.
847	DS200	DS200 Alternate LCD Backlight Inverter	Optional	No	Yes - EMC	
000529	DS200	DS200 carrying case cable, switch, bracket	Optional	Yes	No	
000523	DS200	Double-coated Tape	Optional	Yes	No	
000534	DS200	DS200 Clamp to chassis	Optional	Yes	No	
000535	DS200	DS200 Clamps Chassis Tape & holes	Optional	Yes	No	
000545	DS200	DS200 Image Scanner Cable labels	Optional	Yes	No	Document change
000554	DS200	Mylar tab (double sided tape)	Optional	Yes	No	Document change
000562	DS200	DS200 Mount knurling motor process change	Optional	Yes	No	Document change
000566	DS200	DS200 Labels, screws & clamps	Optional	Yes	No	Document change
000570	DS200	DS200 Wire change black color wires to use different colors	Optional	Yes	No	
000576	DS200	DS200 End of Life SMT Power Inductors	Optional	Yes	No	
000582	DS200	Improve fit of the plastic printer door.	Optional	Yes	No	
000618	DS200	Part number labels- change text on label to identify the hardware revision	Optional	Yes	No	Document change
851	DS200	USB change to the number of the part	Optional	Yes	Yes - Func	
000665	DS200	DS200 ballot box diverter extender field retro-fit	Optional	Yes	Yes - Func	This change did not require any testing however; this was delivered by ES&S as part of the configuration under test.

<b>Change ID</b>	<b>System</b>	<b>Description</b>	<b>Mandatory</b>	<b>De Minimis</b>	<b>Tested</b>	<b>Note</b>
000669	DS200	DS200 Tote Bin	Optional	Yes	Yes - Func	This change did not require any testing however; this was delivered by ES&S as part of the configuration under test.
000628 & 000674	DS200	DS200 Plastic power cord shield and case	Optional	Yes	Yes - Func	This change did not require any testing however; this was delivered by ES&S as part of the configuration under test.
855	M650 Zip Disk	M650 Zip Disks alternate manufacturer	Optional	Yes	Yes - Func	This change did not require any testing however; this was delivered by ES&S as part of the configuration under test.