iBeta
QUALITY ASSURANCE

Appendix E - Discrepancy Report

Prepared for

Premier Election Solutions

Allen, TX 75013
EAC Application # DBD0701

Version 2.0

(V)2009-22Jul-001(B)

U.S. Election Assistance Commission
VSTL

EAC Lab Code: 0702 - Effective thru 2/28/2009 - Renewal Approved by Commissioners - 7/14/2009

NVLAP LAB CODE 200749-0

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

Version History

Ver #	Description of Change	Author	Approved by	Date
v1.0	Initial Release	Gail Audette Dharma Valdez Charles Cvetezar	Gail Audette	22 July 2009
v2.0	Added verbiage on #94, #100, and #131 acceptance	Charles Cvetezar	Gail Audette	29 July 2009

Trademarks

ASSURE®, AccuVote®, AccuVote ES®, AccuView Printer®, BallotStation®, ExpressPoll®, GEMS®, Optical Scan Accumulator Adapter™, Premier Election Solutions®, UAID®, and Key Card Tool™ are trademarks owned by or licensed to Premier Election Solutions.

AutoMARK™ and AIMS™ are trademarks of AutoMARK Technical Systems

PhotoScribe® is a registered trademark of DRS Data & Research Services plc.

All other trademarks are the exclusive property of their respective owners.

TABLE OF CONTENTS

7.5 Discrepancy Report

This report incorporates open discrepancies in the scope of ASSURE 1.2 that were transferred from SysTest at the time of their suspension. The SysTest discrepancy number is reflected in the description. Issues encountered by iBeta during testing are contained in the report. The handling of discrepancies closed by SysTest are reported in the Premier Election Solutions Assure 1.2 Voting System Certification Test Report (Report Number 06-V-DB-058-CTR-01).

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
1	12/19/08	C.Cvetezar	Documentation Defect	Closed	FEC 2002 PCS 2.2.1 Technical Data Package System Maintenance Procedures v1.0 DRS PhotoScribe PS900 iM2/PS960 Hardware Guide v6.0	The Hardware Guide listed (referenced by the System Maintenance Procedures listed) does not address parts by size, manufacturer's designation or individual quantities needed.	v.2: 2.9.4.1 Common Standards- 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: b. Size; d. Manufacturer's designation; e. Individual quantities needed;	[2009-01-23] TT: See section 6, Maintenance, in the DRS PS900 iM2/PS960 Hardware Guide, Rev 7.0. Additional descriptive information has been provided to allow users to easily identify supplies and parts needed to perform maintenance of DRS scanners. Note that DRS maintenance parts are available from Premier on a kit basis. Since the kit is clearly named ("PS900 1 Million Ballot (form) Kit") and described, we do not feel that items within the kit need to be identified by size or manufacturer's designation.	Accepted: GA 5/8/2009: Review of Revision 7 was completed and verified to address the discrepancy.
2	12/31/08	K. Wilson	Documentation Defect	Closed	Assure/GEMS/AIMS/Automark TDP	Reference is made to an "Automark Technical Systems VPN" in "AutoMARK PREM Ballot Scanning and Printing Specification AQS-13-5002-007-S.doc" (Rev. 4) and "AutoMARK PREM Embedded Database Interface Specifications AQS-13-5002-005-S.doc" (Rev. 4). We can find no other references to a VPN in the documentation. The usage of a VPN must be fully described in the documentation in order that we assess the applicability and security testing of these two sections in particular and possibly other sections related to telecommunications and data transmission over public networks. The appearance of the word VPN in the AutoMARK documentation conflicts with the "N/A" that appears in numerous subsections of section 6.5 and 6.6 of the documents "AIMS PREM Sect00C Requirements Trace Matrix AQS-13-5000-203-R.doc" and "AutoMARK PREM Requirement	VSS Volume 1 Section 6.6.1 All systems that transmit data over public telecommunications networks shall: ... and Section 6.6.2 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 poll sites 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.	[2009-01-27] SB: The reference to VPN in both documents is describing the internal company procedure used to transfer and keep source code private. This VPN reference is in no way part of the AutoMARK functionality. It states: " C. Privacy: The embedded database source code is not transferred over the internet except through the Automark Technical Systems VPN."	Accepted: GA 5/18/2009: Review of TDP and equipment as well as operational manuals confirms that the VPN is only used for development and not implementation.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						Trace Matrix AQS-13-5000-003-F.doc"			
3	1/9/09	K. Wilson	Documentation Defect	Closed	Security Review - ExpressPoll (appears in I:2.2.2.1.e, because that is where it was observed)	ExpressPoll, EZRoster "ExpressPoll CardWriter 1.1.6 TDP Appendix A Software Specifications.pdf Rev 1.1" states that the C# application, ExPollCardWriter, and the C++ application, PcmCardDll, are "console" applications running on Windows CE (source code review concurs). The documents "ExpressPoll 2000 EZRoster System Administrators Guide Revision 4.0.pdf" Rev 4.0 and "ExpressPoll 4000 EZRoster Pollworkers Guide Revision 2.0.pdf" Rev. 2.0 show a user interface. We cannot find the source code to this user interface application and also cannot find a reference to it in "ASSURE1 2MatrixRev4 0Nov1708.xls" (Matrix) We do not have any source code for a user interface application that looks like EZRoster nor do we have anything labelled EZRoster, ExPoll or ExPollLauncher. The latter two are referred to in a documents delivered to Systest on 3/23/2007: "ExpressPoll EZRoster 1.0 Build Process Revision 2.0.pdf" and "ExpressPoll EZRoster 2.0 Build Process Revision 1.0.pdf" However we are not sure if these two documents are a part of the current TDP because they do not appear in the Matrix spreadsheet. All three devices, 5000, 4000, and 2000 are included in the Premier application as COTS. The user interface figures in the documentation shows such words as "Diebold Election Systems", "Manage Polls,", "Ballots." Please clarify. Furthermore, the document "ExpressPoll CardWriter 1.1.6 TDP Appendix F Installation Procedures.pdf" states that there is both a Boot Rev 4.7 and CE OS 2.56. We do not have the configuration or source files for either one of these.	I: 9.4.1.3 The software qualification tests encompass a number of interrelated examinations, involving assessment of application source code for its compliance with the requirements spelled out in Volume I, Section 4	[2009-02-24] NF: Volume I, Subsection 9.4.1.3, Focus of Software Evaluation of the 2002 FEC requirements involves the assessment of application source code for its compliance with the requirements spelled out in Volume I, Section 4 as well as functional testing to verify the proper performance of all system functions controlled by the software. These requirements do not address the composition of product documentation used to support the certification submission for the ExpressPoll CardWriter. As it stands, the product documentation submitted in support of the ExpressPoll CardWriter certification effort describes both the functionality of the ExpressPoll CardWriter as well as the EZRoster application - any material referenced in this documentation will be sufficient to demonstrate compliance with the relevant FEC requirements for the ExpressPoll CardWriter software. The ExpressPoll EZRoster 1.0 Build Process Revision 2.0 and ExpressPoll EZRoster 2.0 Build Process Revision 1.0 are no longer applicable, and have been superseded by ExpressPoll CardWriter 1.1 Build Process Revision 9.0.	Accepted: GA 5/18/2009: EZRoster is not part of the Premier application to the EAC (and ExpressPoll 2000 has been removed).
4	1/28/09	K.	Docum	Clos	ASM - TDP	A) No procedure whereby	I: 2.2.1.f - If access to a system	[2009-02-03] NF: A) The issuer	Rejected: KGW

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
		Wilson	entation Defect	ed		jurisdictional level certificates are created and signed by the root certificate. ASM 1.2.1 TDP Appendix B Program Specifications.pdf contains a Use case entitled "Issue new certificates." However ASSURE_Security_Manager_1.2_Users_Guide.pdf contains no such use case. (Nor can it be found in the application). Without this procedure the jurisdiction cannot generate its own certificates, the private key of which it owns. B) Related but also applicable to 6.2.1.f The test application submitted by Premier has a "Premier Root Certificate Authority" which is signing other certificates to provide trust chains. Cannot find any documentation of Premier's internal security policy relating to the physical protection of this root certificate's private key, separation of duties in terms of its usage, or methods to notify the EAC or jurisdictions if the private key is compromised. The security trade-offs associated with the usage of the "Premier Root Certificate Authority" are not discussed in the vendor documentation. The design of the system requires that the jurisdiction install this root certificate as trusted, and thus the procedures associated with its security are appropriate to the EAC and the jurisdictions. Rejected: 5/27/2009 KGW -- The Premier Root Certificate Authority certificate must be associated with a "private" key. What internal controls does Premier enforce to prevent this "private" key from (for example) being posted to the internet.	function is to be restricted or controlled, the system shall incorporate a means of implementing this capability. I:6.2.1.1.f - General characteristics of supervisory access privileges; KGW 5/27/2009 added -- V1: 6.2.1.2.a. Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access V1: 6.2.2.a Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include: a. Use of data and user authorization	certificate provided by Premier Election Solutions is created and signed by Premier - this certificate must currently be imported into ASM, and it is provided in signed form to the client jurisdiction. A certificate is automatically issued by the ASSURE Security Service for every user that is created, as documented in the section Certificates in section 3.3, The ASM namespace interface in the ASSURE_Security_Manager_Users_Guide_1.2.2_or_later_Rev_2.0. User certificate issuance functionality is documented in section ClssueCertProgressDlg in ASM 1.2.1 TDP Appendix B: Program Specifications. No requirement exists in the 2002 FEC voting system standards to discuss security trade-offs associated with the usage of particular root certificates in vendor documentation. [2009-07-07] SL: Premier is ISO 9001 certified and we adhere to our internal procedures for protection of the private key.	5/27/2009 Accepted: GA 7/7/2009: iBeta has received confirmation of Premier's ISO 9001 certification and has witnessed the process of obtaining and protecting the private key as part of the Trusted Build.
5	1/28/09	S. Jakileti	Documentation Defect	Closed	AutoMARK PREM System Security Specification AQS-13-	No referred section 5 in" AutoMARK PREM System Security Specification AQS-13-5002-001-S",No documentation for mandatory administrative procedures (Vol 1 Sec 2.2.2.1 is complete, Vol 1 sec	Vol 1 :2.2.1e:Provide security provisions that are compatible with the procedure and administrative tasks involved in equipment preparation, testing, and operation. Vol 1 :2.2.1g:Provide documentation	[2009-5-19] PH: 2.2.1.e : 2.2.1.g: Trace Matrix points to document System Security Test Procedures AQS-13-5012-000-S and test location System Security	Rejected: GA 5/25/2009 Partial Acceptance: GA 6/18/2009: Review of the

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
					5002-001-S	2.2.3 is incomplete, Vol 1 Sec 6.2.1.1 is incomplete), and no documentation is provided for effective password management. Rejected: GA 5/25/09: The requirements are for documentation of procedures and Test Procedures/Cases do not meet this requirement.	of mandatory administrative procedures for effective system security. Vol 1 :2.2.3a:Restoration of the device to the operating condition existing immediately prior to the error or failure, without loss or corruption of voting data previously stored in the device; Vol 1 :2.2.3b:Resumption of normal operation following the corrections of a failure in a memory component, or in a data processing component, including the central processing unit; Vol 1 :6.2.1d:Effective password management;	Test Case AQS-13-5030-005-S. 2.2.3.a: Trace matrix points to Operations and Diagnostic Log Specs AQS-13-5002-004-S and test case location Operation Log Test Cases AQS-13-5032-005-S 2.2.3.b: Trace matrix points to System level test cases AQS-13-5030-000-F 6.2.1.d: Trace Matrix points to System Security Specification AQS-13-5002-001-S in section 2.B and 2.C [2009-6-02] PH: 2.2.1.e: 2.2.1.g: Added Section 2.C.2.1 to AutoMARK PREM System Security Specification AQS-13-5002-001-S.doc 2.2.3.a: 2.2.3.b: Added Section 2.E to the above document. 6.2.1. Added section 2.B.1.c to the above document.	AutoMARK System Security Specifications Revision 4 dated 6/01/09 addressed the Vol1: 2.2.1g, 2.2.3a, and 2.2.3b portion of the discrepancy; however, requirements 2.2.1e, and 6.2.1d are still pending response from Premier. Accepted: GA 6/30/09: Review of the AutoMARK TDP received on 6/29/09 verified compliance with the requirement.
6	1/28/09	S. Jakileti	Documentation Defect	Closed	AccuVote-TSX with AVPM TDP Appendix D: COTS Component Specifications	Not finding referenced document "AccuVote-TSX with AVPM TDP Appendix D: COTS Component Specifications" in 08062008 delivery	vol 1 2.2.4.1e: Protect against the failure of any data input or storage device;	[2009-02-02] NF: This documentation should have been included with the AccuVote-TSX with AVPM TDP delivery. This appendix will be sent to the VSTL.	Accepted: GA 5/18/09: This document was delivered as part of the TDP on 5/18/09.
7	1/28/09	S. Jakileti	Documentation Defect	Closed	AccuVote-OS Central Count TDP	Documented as recording normal and abnormal events as out of scope and address by the controlling application (when no connection to the host has been established, where the events are logged)	vol1 2.2.4.1g:Record and report the date and time of normal and abnormal events; vol1 2.2.4.1i: 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;	[2009-02-03] NF: The AccuVote-OS device acts as a dumb scanner, and represents one component of the Central Count system. The AccuVote-OS scanner is controlled by either GEMS or PCS, applications which provide system logic, and amongst others, audit functionality.	Accepted: KGW 5/27/2009 as per vendor response
8	1/28/09	S. Jakileti	Documentation Defect	Closed	AccuVote-OS Precinct Count TDP	No protection procedures are provided against the failure of any data input or storage device (documented in the AVOS TDP as out of scope, but the data is stored on the memory card)	vol1 2.2.4.1e: Protect against the failure of any data input or storage device;	[2009-02-03] NF: This information is provided in section 2.3.2.4.1, Common Standards (e) in AccuVote-OS TDP 2.03 System Functionality Description in the AccuVote-OS TDP.	Accepted: GA 5/18/2009: Review of documentation determined that the memory card is addressed.
9	1/28/09	S.	Docum	Clos	Security	No protection procedures are	vol1 2.2.4.1e: Protect against the	[2009-02-03] NF: This information	Accepted: GA

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
		Jakileti	entation Defect	ed	review-AccuVote-AVOSX TDP	provided against the failure of any data input or storage device (documented in the AVOSX TDP as out of scope, but the data is stored on the memory card)	failure of any data input or storage device;	is provided in section 2.3.2.4.1, Common Standards (e) in AccuVote-OSX TDP 2.03 System Functionality Description in the AccuVote-OSX TDP.	5/18/2009: Review of documentation determined that the memory card is addressed.
10	1/28/09	K. Wilson	Documentation Defect	Closed	Premiers Client Security Policy.pdf Rev 3.0	Premiers Client Security Policy.pdf Rev 3.0 -- Document does not contain a description in sufficient detail to allow an unskilled user to set the password history (2.3.1) or password aging (2.3.2) requirements in the COTS OS. Doc P: Document does not contain a description in sufficient detail to allow an unskilled user to set the audit log security policies of a COTS OS.	v1: 2.1.1.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.		Accepted: KGW 3/24/2009: Windows Configuration Guide Rev 6 (delivered on 03/04/09) contains this information and closes out the discrepancy prior to a formal response from the vendor.
11	1/28/09	K. Wilson	Documentation Defect	Closed	Premiers Client Security Policy.pdf Rev 3.0	Premiers Client Security Policy.pdf Rev 3.0 -- Document contradicts itself. In section 3.1.1 it recommends that passwords should not be shared among users. But in section 3.4.2 it recommends that only a single administrator account exist. If the single administrator does not share the password then in the event that the single administrator is unavailable the system might become inaccessible. 3.1.1 is correct, all users must be individually audited for their actions.	v1: 2.1.1.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.	[2009-02-03] NF: The statement in section 3.4.2, Administrative account privileges 'The number of privileged accounts should be kept to an absolute minimum - preferably, one single account.' has been revised in Premiers_Client_Security_Policy_Rev_4.0.	Accepted: GA 5/22/2009: Based on review of the updated document, this discrepancy is closed.
12	1/28/09	K. Wilson	Documentation Defect	Closed	VCProgrammer TDP	VCProgrammer - Neither "VCProgrammer User's Guide Revision 1.0" nor "VCProgrammer 4.7.2 System Administrator's Guide Revision 1.0" describe the activity which the document VCProgrammer 4.7.2 Technical Data Package Appendix G: System and Data Integrity Revision 1 refers to in section 5.3 (bullet item 5). When does the described activity occur?	v1: 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.	[2009-02-03] NF: The reference to the Central Administrator card has been removed from section 5.3, VCProgrammer in VCProgrammer 4.7.2 TDP Appendix G: System and Data Integrity. This change will be reflected in the VCProgrammer 4.7.2 TDP Revision 2.0.	Accepted: KM 6/2/2009: FEC 2002 VCProgrammer TDP Appendix F: System and Data Integrity, version 1.0 (May 15, 2009) has had the reference removed.
13	1/28/09	K. Wilson	Documentation Defect	Closed	VCProgrammer TDP	VCProgrammer -- Documentation does not address parity or checksums protecting Configuration files accepted from the Voter Card Data File accepted from the external voter registration system.	v1:2.1.2.e Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.	[2009-02-03] NF: The relevant text in section 4, Data Quality Assessment has been amended in VCProgrammer 4.7.2 TDP Appendix G: System and Data Integrity, as well as the smart card format document provided in VCProgrammer 4.7.2 TDP Appendix D: Smart Card Format.	Accepted: KM 6/2/2009: The manual has been updated to state that CRCs are used to protect the files. Source code review by Lauren Laboe confirmed

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
								Error messages listed inVCProgrammer_Users_Guide_4.7.4_or_later_Rev_1.0have also been updated	that this is the case.
14	1/28/09	K. Wilson	Documentation Defect	Closed	VCProgrammer TDP	VCProgrammer -- Documentation does not describe the authentication of the file or system inputing the file "Voter Registration File" The system inputting this information is outside the boundary of the Assure 1.2 certified system, but this external system apparently has access to the VCProgrammer computer with the ability to at least place the file onto the system at an appropriate time. This placement appears to occur dynamically at the time of the voter obtaining a vote access card over a network connection. Rejected: 5/22/09 GA: v1: 6.2 "The access controls contained in this section of the Standards are limited to those controls required of system vendors." As the VCProgrammer is a shared environment with the voter registration system (not part of the certification), the network connection to that shared environments impact on the access control policy and must be addressed in the TDP.	v1: 6.2.1 The vendor shall specify the general features and capabilities of the access control policy recommended to provide effective voting system security.	Premier - iBeta response on 5/22/09 [Nel, 2009-06-10] VCProgrammer TDP Revision 2.0 as well as VCProgrammer 4.7.4 or later User's Guide Revision 2.0 must be delivered.[TT 2009-06-15] Added notes regarding use of VCProgrammer on a LAN. See section 3, Installing VCProgrammer in the VCProgrammer User's Guide 4.7.5 or later Rev 2.0. Added anti-virus software recommendation to Premier's Windows Configuration Guide Rev 10.0.	Rejected: GA 5/22/2009 Accepted: GA 6/18/09: Review of the VCProgrammer System Adminstrator's Guide 4.7.5 or later Revision 1.0 dated June 15, 2009, Section 3.0 verifies that the TDP addresses the installition of VCProgrammer on a LAN and Premier's Windows Configuration Guide Revision 10 dated Jun 15, 2009 Section 3.2.1 verifies that the TDP addresses the recommendation for anti-virus software.
15	1/28/09	K. Wilson	Documentation Defect	Closed	GEMS 1.21.1 Election Administrator's Guide Rev 2.0	The first paragraph of section 12.3 states that each task falls within corresponding personnel categories and lifecycle component. However the document does not tie each task with any particular personnel category or lifecycle component. It likewise does not address how the personnel categories in section 12.1 overlap or intersect with the roles imposed by the Key Card Tool. (see also 6.2.1.1.f) This is important information from a security policy perspective (Premier Client Security Policy document reference)	v1: 6.2.1.2.b Specify whether an individual's authorization is limited to a specific time, time interval or phase of the voting or counting operations	[2009-02-03] NF: The requirements upon which this discrepancy has been raised have no bearing on the discrepancy. In fact, the discrepancy should be based on Volume I, Subsection 6.2.1.2, Individual Access Privileges (a), and optionally Volume II, Subsection 2.8.1, Introduction. The response to section 2.6.1.2, Individual Access Privileges in Key Card Tool 4.7.2 TDP 2.06 System Security Specification in fact states 'the recommended functions and data to which each personnel category holds authorized access are detailed in section 12.4, Personnel category/election task assignment in the ...' GEMS	Accepted: KM 6/10/2009: GEMS_Election_Administrators_Guide_1.21.3_or_later_Rev_2.0 has a table relating personnel categories with tasks which also shows overlap.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
								Election Administrator's Guide, which does in fact tie each task with ... particular personnel category or lifecycle components. That said, the GEMS_Election_Administrators_Guide_1.21.3_or_later_Rev_1.0 has been amended to include specific products to which each task listed in section 12.4, Personnel category/election task assignment is applicable to.	
16	1/28/09	K. Wilson	Documentation Defect	Closed	VCProgrammer 4.7.2 TDP 2.06 System Security Specification.pdf	VCProgrammer --As this device may be connected to an untrusted networked device (Voter Registration System) it must be protected by security kernals such as antivirus software and firewalls.	v1: 6.4.2 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.	[2009-02-17] NF: The implementation of firewalls in ASSURE 1.2 PC configurations is documented in section 6.2, Windows Firewall in Premiers_Windows_Configuration_Guide_Rev_8.0. Section 2.6.8.2, Protection Against Malicious Software in VCProgrammer 4.7.2 TDP 2.06 System Security Specification has been amended accordingly.	Accepted: KM 6/3/2009: The Premier Windows Configuration Guide Revision 8 stipulates that a firewall must be used in section 6.2.
17	1/28/09	K. Wilson	Documentation Defect	Closed	VCProgrammer 4.7.2 TDP 2.06 System Security Specification.pdf	VCProgrammer, Assure Security Manager, Key Card Tool, PCS Workstation, GEMS -- Documentation does not cover the required antivirus, firewall or other software and/or security kernels used to protect the system. Consequently it does not provide any published standards used to accept this software. In regards to statements made regarding the usage of the "Microsoft Malicious Software Removal Tool," Microsoft documentation (http://support.microsoft.com/kb/890830) states: "The Microsoft Malicious Software Removal Tool does not replace an antivirus product" so this tool (standing alone) does not meet the "proven commercial security software requirement." Rejected: 6/1/2009 KM: In Process. The issue of anti-virus software is not addressed in the specified document, nor is it addressed in the referenced documents.	v2: 6.4 The ITA may meet these testing requirements by confirming proper implementation of proven commercial security software. In this case, the vendor must provide the published standards and methods used by the US Government to test and accept this software, or it may provide references to free, publicly available publications of these standards and methods, such as government web sites.	[2009-02-17] NF: The implementation of firewalls in ASSURE 1.2 PC configurations is documented in section 6.2, Windows Firewall in Premiers_Windows_Configuration_Guide_Rev_8.0. Section 2.6.8.2, Protection Against Malicious Software in VCProgrammer 4.7.2 TDP 2.06 System Security Specification has been amended accordingly. References to free, publicly available publications of standards and methods employed by Premier in securing election data are included in ASSURE 1.2 TDP Appendix K: SSL Protocol Specification, ASSURE 1.2 TDP Appendix R: AES Encryption Specification, and ASSURE 1.2 TDP Appendix V: SHA1 Specification.	Rejected: KM 6/1/2009 Accepted: GA 6/18/09: Review of the VCProgrammer TDP 2.06 System Security Specification Revision 2.0 dated June 16, 2009, Section 2.6.8.2 verifies that the TDP references the anti-virus software installation recommendation in the Premier's Windows Configuration Guide Revision 10 dated Jun 15, 2009 which in turn in Section 3.2.1 verifies that the TDP addresses the recommendation

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						VCProgrammer TDP 2.06 System Security Specification.pdf, Rev 1.0. May 15, 2009.			for anti-virus software.
18	1/28/09	K. Wilson	Documentation Defect	Closed	VCProgrammer, Assure Security Manager, Key Card Tool, PCS Workstation, GEMS (all PC based devices) TDP	VCProgrammer, -- Approved VSTL test plan Rev. 9 calls for a rootkit scanning mechanism. The only documentation found is the AVValidator documentation, which describes a System Identification Tool relevant to section 5.8 of the Program Manual, but this tool does not address the VCProgrammer, Assure Security Manager, Key Card Tool, PCS Workstation or GEMS host computer systems. iBeta will not attempt to introduce a rootkit. Rootkits are notoriously difficult to remove without re-installation of the operating system and generally might contain security vulnerabilities themselves that increase the risk to the system even though the rootkit itself might be benign. In its place, iBeta is creating a documentation discrepancy against rootkit vulnerable operating systems for Premier to document the usage of it for the VCProgrammer etc. Rejected: 5/21/09 KGW: Neither Premier's Windows® Configuration Guide Rev 8.0 nor Premier's Client Security Policy Rev 4.0 direct the installation of the "Microsoft Windows Malicious software removal tool". Reference to it to meet security access control requirements appear in ASM 1.2.1 Technical Data Package Appendix G: System and Data Integrity, Key Card Tool 4.7.2 Technical Data Package System Security Specification, GEMS 1.21.1 Technical Data Package Appendix H: System and Data Integrity. The language in these is similar to the GEMS Appendix H document which states that "Microsoft Windows Malicious Software Removal Tool installed on GEMS servers" as if the installation is already completed. Yet it was not present.	v2:6.4 At its discretion, the ITA may conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities, employing test procedures approved the NASED Voting Systems Board.	[2009-02-23] NF: The stated requirements of Volume II, Subsection 6.4, Security Testing of the 2002 FEC standards have neither any bearing on vendor system validation documentation nor on testing tools employed, such as the rootkit scanning mechanism referenced. [2009-06-01] NF: References to the Windows Malicious software removal tool have been removed from the stated TDPs.	Rejected: KGW 5/21/2009 Accepted: DEV 06/19/2009: Verified the removed reference to the Microsoft Windows Malicious Software Removal Tool in the Premier's Windows® Configuration Guide Revision 10.0 June 15, 2009 and Premier's Client Security Policy Revision 5.0 June 5, 2009.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
19	1/28/09	K. Wilson	Documentation Defect	Closed	VCEncoder TDP	Neither Premier's Windows® Configuration Guide Rev 8.0 nor Premier's Client Security Policy Rev 4.0 direct the installation of the "Microsoft Windows Malicious software removal tool". Reference to it to meet security access control requirements appear in ASM 1.2.1 Technical Data Package Appendix G: System and Data Integrity, Key Card Tool 4.7.2 Technical Data Package System Security Specification, GEMS 1.21.1 Technical Data Package Appendix H: System and Data Integrity. The language in these is similar to the GEMS Appendix H document which states that "Microsoft Windows Malicious Software Removal Tool installed on GEMS servers" as if the installation is already completed. Yet it was not present.	v1: 2.2.1d Provide safeguards to protect against tampering during system repair, or interventions in system operations, in response to system failure.	[2009-02-04] NF: Physical repair is not applicable to the Voter Card Encoder, as the device is COTS, hence requirement is addressed in terms of electronic and administrative tools used to provide security. Protection against tampering during intervention in system operation in response to system failure is assured by the referenced security features described in section 4, Security Monitoring and Control in Voter Card Encoder 1.3.3 TDP Appendix G: System and Data Integrity, which remain applicable from the occurrence of any of the error conditions documented in Appendix E: Troubleshooting in the Voter Card Encoder 1.3.3 or later Rev 1.0 through to their resolution.	Accepted GA 5/20/2009: Voter Card Encoder 1.3.3 or later Rev 1.0 Appendix F: Troubleshooting does not direct the user to perform any system repair and the response to a system failure is to use another unit and/or notify the election office. Section 7 Maintenance lists the only maintenance procedure as replacing the batteries. Based on this documentation review, this discrepancy is closed.
20	1/28/09	K. Wilson	Documentation Defect	Closed	VCEncoder TDP	VCEncoder - Documentation states that communications is not applicable, but the device contains a serial port and as such security must be addressed. It also communicates with a smart card and communication needs to be addressed. Rejected: KGW 5/27/2009 The device contains a serial port which is a communications portal. Vendor response that this portal is used for firmware updates. Therefore it must have either a policy or complete justification as to why it does not need a policy because it is "inactive at all other times" whatever that might mean. Please elucidate in documentation. Rejected: DEV 06/19/2009: The FEC 2002 Voter Card Encoder TDP System Security Specifications Revision 2.0 June 15, 2009 still does not contain justification as to why the	v1: 6.2.1.1c Communications	[2009-02-23] NF: The requirements of Volume I, Subsection 6.2.1.1, General Access Control Policy - note section reference discrepancy - point to policy requirements. As such, administrative policies pertaining to communications are of issue, not functional aspects of communication between the Voter Card Encoder application and the smart card. The Voter Card Encoder serial port is used for firmware updates but is inactive at all other times. The Voter Card Encoder smart card reader is designed to only recognize validly formatted smart cards, encoded with the same smart card key as the Voter Card Encoder. Revised section 7.2.2, Equipment security in Premier's Client Security Policy, rev 6.0	Rejected: KGW 5/27/2009 Rejected: DEV 06/19/2009 Accepted: GA 6/29/2009: Based on review of sections 2.6.1.1, 2.6.2, and 2.6.4 of Voter Card Encoder System Security Specification Revision 3.0 dated June 26, 2009 closes this discrepancy. The TDP added a tamper proof seal on the serial port.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						Voter Card Encoder serial port is inactive at all other times besides firmware updates.		Added: "To prevent unauthorized access to the firmware on the Voter Card Encoder, ensure that a tamper proof seal is applied over each Voter Card Encoder's serial port."	
21	1/28/09	K. Wilson	Documentation Defect	Closed	VCEncoder TDP	VCEncoder -- Unable to find the document "Appendix C: Installing the Firmware in the Voter Card Encoder User's Guide" referred to in "VCE 1.3.3 TDP Appendix A Software Specifications.pdf"	v1: 6.2.1.1.e Protection abilities of a particular operating system;	[2009-02-05] NF: Appendix C: Installing the Firmware is definitely present in the Voter Card Encoder 1.3.3 or later Rev 1.0.	Accepted: GA 5/20/2009: Voter Card Encoder 1.3.3 or later Rev 1.0 Appendix C: Installing the Firmware was received. Based on this documentation review, this discrepancy is closed.
22	1/28/09	K. Wilson	Documentation Defect	Closed	VCEncoder TDP	VCEncoder -- Unable to find the information appropriate to make a determination that an off-the-shelf COTS Spyrus PAR 2 cannot be used to program smart cards to allow unregistered ballots to be cast or that (6.4.1.c) no Spyrus firmware is operational in the absence of the Premier code.	v1: 6.2.1.1.f General characteristics of supervisory access privileges; v2: 2.6.2 Access Control Measure The Vendor shall provide a detailed description of all system acccess 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 reuirement of Volume I, Section 6.2.2.	[2009-02-24] NF: The requirements of Volume I, Subsection 6.2.1.1, General Access Control Policy - note section reference discrepancy - point to policy requirements, not functional requirements.	Accepted GA 5/20/2009: Voter Card Encoder 1.3.3 or later Rev 1.0 Appendix C: Installing the Firmware was received and the access to this environment is stated to be restricted to authorized personnel but the documentation does not state that this is protected against. As a result, this will be tested in the Security Test Case and is closed as a documentation discrepancy.
23	1/28/09	K. Wilson	Documentation Defect	Closed	VCEncoder TDP	VCEncoder -- Cannot find a description of the protocol used to program ballots or the protocol used to download new firmware. "VCE 1.3.3 TDP 2.06 System Security Specification.pdf" states that "Special Protocols" is N/A.	v1: 6.2.1.1.f General characteristics of supervisory access privileges; v2: 2.6.2 Access Control Measure The Vendor shall provide a detailed description of all system access control measures and mandatory procedures designed to permit access to system states in	[2009-02-24] NF: FEC 2002 Volume I, Subsection 6.2.2, Access Control Measures mandates the provision of examples, rather than exhaustive responses to every item listed, hence a targeted response should not have to be provided. The	Accepted: GA 6/18/2009: Review of Voter Card Encoder TDP System Security Specification Revision 2.0 dated June 15, 2009

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						5/20/09 GA: The TDP referenced states that special protocols are not applicable to the Voter Card Encoder since it is not used to communicate with an external electronic device. The COTS Spyrus PAR 2 loads firmware through the COM1 port of an IBM compatible host computer (external electronic device).	accordance with the access policy, and to prevent all other types of access to meet the specific requirement of Volume I, Section 6.2.2.	response to this requirement as provided in section 2.6.2, Access Control Measures in VCE 1.3.3 TDP 2.06 System Security Specification already provides examples of measures used to control access to the Voter Card Encoder application and data. [Nel, 2009-06-02] Section 2.6.2, Access Control Measures (f) in VCE TDP 2.06 System Security Specification has been amended to state 'A COTS protocol is used by the Spyrus PAR 2 for the purpose of loading firmware from an external electronic device onto the Voter Card Encoder.'	verified that the protocol is not listed within this TDP.
24	1/28/09	K. Wilson	Documentation Defect	Closed	VCEncoder TDP	VCEncoder -- "VCE 1.3.3 TDP 2.06 System Security Specification.pdf" does not address this requirement	v1: 6.4.1.c The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as computer chip) other than the component on which the operating system resides; and	[2009-02-04] NF: The Voter Card Encoder firmware - which incorporates device control functionality - is resident in flash storage, whereas election-specific programming is stored in the EPROM firmware.	Accepted: GA 5/20/2009: The TDP states, in Voter Card Encoder 1.3.3 or later Rev 1.0 Appendix C: Installing the Firmware that only the firmware is uploaded to the Voter Card Encoder unit. Although not specifically stated in the TDP, the Vendor Response is accurate and satisfies this requirement.
25	1/28/09	K. Wilson	Documentation Defect	Closed	ExpressPoll TDP	ExpressPoll - Documentation does not address 2.2.1.d which would include the possibility that the device contains PII of voters at the time of failure. Rejected: 6/1/09 GA: Concern is protecting the privacy of the voter per HAVA 301A which is within the safeguards of the VSS requirement cited. Rejected: 6/3/09 KGW -- documentation does not address the privacy of voter PI that might reside	2.2.1.d Provide safeguards to protect against tampering during system repair, or interventions in system operations, in response to system failure.	[2009-06-02] NF: Management of the integrity of voter registration system data is outside the scope of the ExpressPoll CardWriter TDP.	Rejected: GA 6/1/2009 Rejected: KGW 6/3/2009 Accepted: GA 6/26/2009: With the closure of #104 per the EAC instruction to not use the ExpressPoll Updater.cab, this discrepancy is also

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						on the ExpressPoll in case of a system failure. Once such data is loaded onto a certified device it becomes the responsibility of Premier to protect. Therefore documentation must address this point.			closed.
26	1/28/09	K. Wilson	Documentation Defect	Closed	Premiers Client Security Policy.pdf Rev 3.0	Premier Client Security Document - Document does not use the word "mandatory" for any administrative procedures relating to effective system security but instead uses the word "should" which is not the same intent as the requirement "mandatory"	v1: 2.2.1.g Provide documentation of mandatory administrative procedures for effective system security.	[2009-02-04] NF: All Premier Election Solutions product and TDP documentation has been amended to mandate administrative procedures relating to effective system security.	Accepted: KM 6/1/2009 KM: The statement that certified systems must follow the best practices explained in the configuration guides is sufficient. Premiers Client Security Policy.pdf. Rev 4.0.
27	1/28/09	K. Wilson	Documentation Defect	Closed	ExpressPoll CardWriter 1.1.6 TDP 2.06 System Security Specification.pdf	Document states that Communications is N/A which is incorrect. The ExpressPoll units contain USB ports, and Ethernet ports, so communications over these ports must be described. Rejected: 6/3/09 KGW: The policy recommended for communications over these ports must be described. N/A is still unacceptable.	v1: 2.6.2 Access Control Measures that refers to v1: 6.2.1.1.c Communications	[2009-02-23] NF: The requirements of Volume I, Subsection 6.2.1.1, General Access Control Policy - note section reference discrepancy - point to policy requirements, not functional requirements. Hence discussion of communication over ExpressPoll ports is not appropriate here.	Rejected: KGW 6/3/2009 Accepted: GA 6/29/2009: Review of Express Poll CardWriter TDP 2.06 System Security Specification Revision 2.0 dated June 26, 2009 confirmed that the communications is no longer N/A and the reference to the Premier Network Security Guide for the ports (Section 2.6.1.1) and the protocol for communicating with the smart cards (Section 2.6.2) addresses the requirement.
28	1/28/09	K. Wilson	Documentation Defect	Closed	ExpressPoll CardWriter 1.1.6 TDP Appendix F Installation Procedures.pdf Rev 1.0	The requirement is to validate the ROM. The document does not describe validating the ROM. It only validates functionality or a version number. AVValidator does not currently address these devices (4000 or 5000).	v1: 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;	[2009-02-05] NF: This requirement is not actually applicable to the ExpressPoll CardWriter, since it is not technically firmware, resident on a ROM on the ExpressPoll. [2009-06-02] NF: The ExpressPoll	Rejected: GA 5/22/2009 Accepted: KM 6/4/2009: Section 5.7 of the ExpressPoll

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						Rejected: 5/22/09 GA: Section 1.4 states the the "The Firmware will be the last number listed under ROM version." and in Section 2.3 "The OS rev is diplayed as the Rom Version." No other validation is documented.		CardWriter software is not loaded on the referenced ROM. Nonetheless, references in the TDP to ExpressPoll CardWriter TDP Appendix E: Installation Procedures have been replaced with section 5.7, Installing a New Version in ExpressPoll Administrators Guide for Version 2.0 and 2.1. ExpressPoll CardWriter TDP Appendix E: Installation Procedures has been removed from TDP.	Administrator's Guide Version 2.0 and 2.1 references software instead of firmware.
29	1/28/09	K. Wilson	Documentation Defect	Closed	ExpressPoll CardWriter 1.1.6 TDP 2.06 System Security Specification.pdf Rev 2.0	Updated 5/22/09 GA: Requirements which are for all voting system components are not addressed in the TDP per the v2: 2.64 requirements that require meeting the specific requirements of Volume I, Section 6.4. Rejected: 6/3/09 KGW - Taken individually, each item appears to satisfy the requirement. As a whole the information is contradictory and possibly incorrect. As we have come to understand it, the ExpressPoll firmware is upgradeable through loading the appropriate CF and a Supervisor or Administrator Smart Card (with PIN). That does not qualify as "permanently resident" The TDP at 6.4.1.a states that the software is not on a ROM but then that assertion is contradicted in 6.4.1.c by stating that the firmware is permanently resident (which implies ROM). We now understand that installation of the firmware does not include the OS and/or the bootloader. Please direct us to the documentation which supports the concept that COTS OS and bootloader are "permanently resident" if that is the case (ref vol 2:2.2.1.5 the information of which was also not found in sufficient detail to meet the documentation requirements in "ExpressPoll CardWriter Technical Data Package System Overview" Rev May 19,	v1: 6.4.1.c The 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; and v1: 6.4.1.d The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as computer chip) other than the component on which the operating system resides; and and v1: 6.4.1.e After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible.	2009-02-05] NF: With respect to c), system bootstrap and monitor functionality is provided by the COTS ExpressPoll bootloader. Device control functionality lies in the domain of the Windows CE operating system. The ExpressPoll CardWriter is not used for vote counting purposes. The existing responses to d) and e) are valid. [2009-06-02] NF: The responses previously provided satisfy the referenced requirements.	Rejected: KGW 6/3/2009 Accepted: GA 6/29/2009: Review of Express Poll CardWriter TDP 2.06 System Security Specification Revision 2.0 dated June 26, 2009 confirmed that the bootstrap and monitor functionality is documented in Section 2.6.4.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						2009)			
30	1/28/09	K. Wilson	Documentation Defect	Closed	ASM 1.2.1 TDP 2.03 System Functionality Description.pdf	ASM 1.2.1 TDP 2.03 System Functionality Description.pdf section 2.3.2.1.5 contains all "should perform" procedures not mandatory procedures per the VSS requirement.	v1: 2.2.1.g Provide documentation of mandatory administrative procedures for effective system security.	[2009-02-04] NF: All Premier Election Solutions product and TDP documentation has been amended to mandate administrative procedures relating to effective system security.	Accepted: KM 6/1/2009: Section 2.3.2.1.5 has been updated to state that the best practices listed in the Client Security Policy guide are mandatory. ASM TDP 2.03 System Functionality Description.pdf. Rev 1.0. May 19, 2009.
31	1/28/09	K. Wilson	Documentation Defect	Closed	ASM 1.2.1 TDP Appendix G System and Data Integrity.pdf	Document does not state what files, folders, and databases the ASM subsystem and/or PCS require for jurisdictions to archive or backup from an election.	v1: 2.2.1.g Provide documentation of mandatory administrative procedures for effective system security.	[2009-02-06] NF: A procedure for backing up and restoring the PCS workspace is provided in section 11, Creating and Restoring a Backup Workspace in the PCS_Users_Guide_2.2.2_or_later_Rev_2.0. A procedure for backing up and restoring the ASS database is provided in section 6, Creating and Restoring a Backup in the ASSURE_Security_Manager_Users_Guide_1.2.2_or_later_Rev_2.0.	Accepted: GA 5/22/2009: Section 11 of the Premier Central Scan User's Guide 2.2.2 or later revision 1.0 and Section 6 of the ASSURE Security Manager User's Guide 1.2.2 or later revision 2.0 were reviewed and this discrepancy is closed.
32	1/28/09	K. Wilson	Documentation Defect	Closed	ASM 1.2.1 TDP Appendix G System and Data Integrity.pdf revision 1.0	Section 5.4 refers to integrity supported by OpenGroup DCOM. However the build document "ASSURE Security Service 1.2 Build Process Revision 1.0.pdf" does not include any such COTS subsystem. If system utilizes Microsoft DCOM then Microsoft references are required to support any integrity, confidentiality or authenticity claims. Rejected: 5/25/09 GA: It is understood that the Windows DCOM layer performs data validation. The requirement is that whatever is utilized contains control logic and data processing methods incorporating parity and check-sums (...see requirement). The referenced document for this requirement within the Premier TDP is an Open Group Remote Procedure Call written in	v1: 2.2.1.d Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy, and	[2009-02-06] NF: DCOM is a feature of Windows, for which no special reference is necessary in the build process document, as it is not used to performed the build, nor needs to be explicitly installed as part of the product. [2009-06-04] NF: Section 2.3.2.2.1, Common Standards in ASM TDP 2.03 System Functionality Description has been redacted to indicate that evidence of control logic incorporating parity or check-sums to demonstrate that the system has been designed for accuracy is provided in the section Identifying the caller: Authentication in the web link describing DCOM, msdn.microsoft.com/en-us/library/ms809311.aspx#dcomarch_secdis	Rejected: GA 5/25/2009 Accepted: GA 6/19/2009: Based on review of ASM TDP 2.03 System Functionality Description Revision 2 dated June 26, 2009, in Sections 2.3.2.2.1 and 2.3.2.4.1, the reference to the broken link is removed and replaced with information that addresses the requirements.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						1997 and does not demonstrate that the system has been designed for accuracy.			
33	1/28/09	K. Wilson	Documentation Defect	Closed	ASM 1.2.1 TDP 2.03 System Functionality Description.pdf revision 1.0	ASM 1.2.1 TDP 2.03 System Functionality Description.pdf states that this requirement is N/A. It is the responsibility of the software to determine the degree of operability of the hardware upon which it relies for functionality and may include 1) ability to verify operability of the write/read audit log file 2) ability to verify operability of DCOM and/or other systems communications 3) ability to verify operability of a biometric security device Rejected: 5/25/09 GA: If this is not N/A then the TDP should reflect the correct reference.	v1: 2.2.4.1.j Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability.	[2009-02-06] NF: Self-test and diagnostic functionality for the purpose of detecting and reporting the system's status and degree of operability is achieved by executing an acceptance test upon receipt of the software from Premier Election Solutions. This acceptance test is documented in section 7, Acceptance Test in the ASM User's Guide. [2009-06-01] NF: Section 2.3.2.4.1, Common Standards in ASM TDP 2.03 System Functionality Description has been amended to state that verification of ASM functionality following product receipt is performed procedurally with the execution of the acceptance test documented in section 7, Acceptance Test in the ASM User's Guide. Verification of auditing, transmission, and fingerprint scanner functionality is addressed, either explicitly or implicitly, in the referenced acceptance test.	Rejected: GA 5/25/2009 Accepted: GA 6/19/2009: Based on review of ASM TDP 2.03 System Functionality Description Revision 2 dated June 26, 2009, in Sections 2.3.2.2.1 and 2.3.2.4.1, the information that addresses the requirement is provided in place of the N/A.
34	1/28/09	K. Wilson	Documentation Defect	Closed	ASM 1.2.1 TDP Appendix A Software Specifications.pdf revision 1.0	ASM 1.2.1 TDP Appendix A Software Specifications.pdf states that the ASM software runs on "Windows NT." What versions of NT are supported? Other documents imply the possibility that it can run on XP, Windows Server 2000, Windows Server 2003. (also 6.2.1.b) The EAC Application is only for Windows XP.	v1:6.2.1.a Software Access Controls	[2009-02-25] NF: Reference to Windows NT has been removed from ASM 1.2.1 TDP Appendix A: Software Specifications. References to the operating system supporting ASM have been brought into consistency with the sanctioned operating systems listed in the ASSURE 1.2 Matrix (ie. Windows XP).	Accepted: KM 6/3/2009: The ASM TDP Appendix A: Software Specifications Revision 1 (May 20, 2009) document only lists Windows XP for operating systems that ASM runs on.
35	1/28/09	K. Wilson	Documentation Defect	Closed	Premier's Windows Configuration Guide Rev 4.0Draft.pdf	Premier's Windows Configuration Guide Rev 4.0Draft.pdf does not delineate what systems need to have the configuration performed on them and this document is not addressed in all Windows platform software security documentation.	v1:6.2.1.1.b Hardware access controls	[2009-02-23] NF: Section 1.1, Scope of the Premiers_Windows_Configuration_Guide_Rev_8.0 has been amended to state that the document 'is recommended by Premier Election Solutions for use with all of Premier's non-	Accepted: GA 5/25/2009: Based on review of the delivered Revision 8.0 of the Premier's Windows Configuration Guide, this

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
								embedded software applications'.	discrepancy is closed.
36	1/28/09	K. Wilson	Documentation Defect	Closed	ASM 1.2.1 TDP 2.04 System Hardware Specification.pdf revision1.0	ASM 1.2.1 TDP 2.04 System Hardware Specification.pdf does not address the fingerprint scanners that are compatible with ASM or their interoperability. 5/25/09 GA: The requirement is that the vendor shall provide a description of recommended policies for hardware access controls. The fingerprint scanners are not addressed (compability or interoperability) with the ASM in the hardware specification. Rejected: 6/4/2009 KM: Section 7 of Premier's Client Security Policy (Revision 4.0, April 20, 2009) describes physical security of sensitive hardware based on storing the equipment in secure rooms and logging all access to the storage rooms. It does not address fingerprint scanners or interoperability with ASM.	v1:6.2.1.1.b Hardware access controls	[[2009-06-02] NF: Section 7, Physical Security Practices in Premier's Client Security Policy, referenced in section 2.6.1.1, General Access Control Policy (b) in ASM TDP 2.06 System Security Specification, does in fact describe hardware access control policy applicable to ASSURE 1.2 voting devices as well as ancillary voting equipment, such as the ASM fingerprint scanner. Section 7, Compatibility in ASM TDP Appendix A: Software Specifications has been amended to include a statement to the effect that the fingerprint scanner employed by ASM is compatible with the Windows environment in which ASM operates as well as the USB port specifications of the ASM server. Access control functionality provided by the fingerprint scanner itself is documented in section 3.3.6, Adding fingerprint scans to users in the ASM User's Guide.	Rejected: KM 6/4/2009 Accepted: DEV 06/22/2009: Verified section 3.3.6 of the ASSURE Security Manager User's Guide 1.2.3 or later, sections 4.2 and 5.1 of the FEC 2002 ASSURE Security Manager Technical Data PackageSystem Security Specification Revision 1.0 and the reference made to ASM Appendix K Hardware Specifications all contained information in regard to the fingerprint scanner.
37	1/28/09	K. Wilson	Documentation Defect	Closed	ASM 1.2.1 TDP 2.04 System Hardware Specification.pdf revision1.0	ASM 1.2.1 TDP 2.04 System Hardware Specification.pdf (as in 6.2.1.a) No hardware or COTS platform is specified. Running this software on a peer-to-peer network creates security problems not addressed in vendor documentation. See http://support.microsoft.com/kb/266625. (Authentication of DCOM utilizing a peer-to-peer network). Rejected: 6/3/09 KGW -- I have since discovered that the above concern is handled by the password of the ASSURE_USER. Please document how the jurisdiction sets this password and/or refer to that documentation in this section.	v1: 6.2.1.1.d Effective password management;	[2009-02-24] NF: The requirements of Volume I, Subsection 6.2.1.1, General Access Control Policy (d) - note section reference discrepancy - point to password management policy requirements, and not to hardware documentation requirements or network configuration requirements. [2009-06-15] TT: Added instructions on how to set the password for the ASSURE 1.2 User in the ASSURE Security Manager User's Guide 1.2.3 or later Rev 4.0.	Rejected: KGW 6/3/2009 Accepted: SS 6/17/2009: Based on review of the updated TDP, this discrepancy is closed.
38	1/28/09	K. Wilson	Documentatio	Closed	ASSURE_Security_Manager	ASSURE_Security_Manager_1.2_Users_Guide.pdf has the supervisor	v1: 6.2.1.1.d Effective password management;	[2009-02-24] NF: The requirements of Volume I,	Accepted GA 5/25/2009:

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
			n Defect		_1.2_Users_Guide.pdf	creating a new user with a password (3.3.5.10). Cannot find here or in PCS_2.2.1_Users_Guide_Rev_1.0.pdf any way for the new user to change their password. Unless there is biometric enrollment, the supervisor can impersonate any other user on the system.		Subsection 6.2.1.1, General Access Control Policy (d) - note section reference discrepancy - point to password management policy requirements, and not to password management requirements.	Premier Central Scan User's Guild 2.2.2 or later revision 1.0 contains added section 4.7, Change my password. Based on review of the updated TDP, this discrepancy is closed.
39	1/28/09	K. Wilson	Documentation Defect	Closed	Assure Security Manager TDP	Unable to find any reference to what fingerprint scanner/readers are compatible with ASM and PCS. Rejected: 5/25/09 GA: COTS must be specified in the TDP. Rejected: 6/4/2009 KM: Section 5/2 of ASSURE Security Manager TDP Appendix G: System and Data Integrity states that a fingerprint can may be required for logon, but it does not specify a brand or model of COTS fingerprint reading device that can be used	v1: 6.2.1.2.a Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access v1: 9.3 The hardware submitted for qualification testing shall be equivalent, in form and function, to the actual production versions of the hardware units or the COTS hardware specified for use in the TDP.	[2009-02-25] NF: The stated requirement does not call for the documentation of ancillary hardware components used in tandem with the applications in question. [2009-06-01] NF: Specifications for the fingerprint reader (or equivalent) supported by ASM are provided in the folder Fingerprint reader in ASM TDP Appendix K: Hardware Specifications. [2009-06-01] NF: Section 2.6.2, Access Control Measures (d) in ASM TDP 2.06 System Security Specification has been amended to indicate that ASS/ASM security kernels are documented in section 5, Security Monitoring and Control in ASM TDP Appendix G: System and Data Integrity. Section 5, Security Monitoring and Control in ASM TDP Appendix G: System and Data Integrity does not discuss SSL functionality, since it is not used by ASM to transmit to PCS workstations, rather, DCOM is, for which a description of authentication and encryption functionality is referenced section 5.6, Transmission. The securing of smart cards as well as the manner in which smart cards enhance application security are in fact applicable, and are documented in section 5.5, Security tokens. Default fingerprint reader FRR and FAR ratios are documented in	Rejected: GA 5/25/2009 Rejected: 6/4/2009 KM Accepted: SS 06/15/2009: The reference to what fingerprint scanners/readers are compatible with ASM and PCS is now included in ASSURE Security Manager User's Guide 1.2.3 or later Revision 1.0 June 15, 2009

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
								Appendix B: Fingerprint Reader FRR and FAR ratios in the ASM User's Guide.	
40	1/28/09	K. Wilson	Documentation Defect	Closed	ASM 1.2.1 TDP 2.06 System Security Specification.pdf	ASM 1.2.1 TDP 2.06 System Security Specification.pdf states that this requirementis N/A. In fact the documentation needs to address such things as a) underlying security kernels associated with the SSL claimed to be in operation between the workstations and ASM (is this OpenSSL, Windows or some other kernel?) b) security kernels associated with the smart card security. c) this would be a good place to address the biometric security kernel which would include its default or not default operational settings and such things as the FRR and FAR and/or if this is under jurisdictional control somewhere. 5/27/2009 KGW V1: 6.2.2 "Vendors shall provide a detailed description of all system access control measures." Smart cards not used in ASM. Otherwise please use this section or some other appropriate section to address a) and c)	v1: 6.2.1.2.d Security Kernels	[2009-02-25] NF: FEC 2002 Volume I, Subsection 6.2.2, Access Control Measures - note corrected section reference - mandates the provision of examples, rather than exhaustive responses to every item listed, hence a targeted response should not have to be provided. The response to this requirement as provided in section 2.6.2, Access Control Measures in ASM 1.2.1TDP 2.06 System Security Specification already provides examples of measures used to control access to the ASM application and data. [2009-06-01] NF: Section 2.6.2, Access Control Measures (d) in ASM TDP 2.06 System Security Specification has been amended to indicate that ASS/ASM security kernels are documented in section 5, Security Monitoring and Control in ASM TDP Appendix G: System and Data Integrity. Section 5, Security Monitoring and Control in ASM TDP Appendix G: System and Data Integrity does not discuss SSL functionality, since it is not used by ASM to transmit to PCS workstations, rather, DCOM is, for which a description of authentication and encryption functionality is referenced section 5.6, Transmission. The securing of smart cards as well as the manner in which smart cards enhance application security are in fact applicable, and are documented in section 5.5, Security tokens. Default fingerprint reader FRR and FAR ratios are documented in Appendix B: Fingerprint Reader FRR and FAR ratios in the ASM User's Guide.	Rejected KGW 5/20/2009 Accepted: KGW 6/3/2009: Documented as described
41	1/28/09	K. Wilson	Documentatio	Closed	ASM 1.2.1 TDP 2.06	ASM 1.2.1 TDP 2.06 System Security Specification.pdf states that	v1: 6.2.1.2.g Message encryption and	[2009-02-25] NF: The DCOM tool used to perform remote object	Rejected: GA 5/25/2009

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
			n Defect		System Security Specification.pdf revision 1.0	encryption is used but provides no details. 5/25/09 GA: The details provided in the response to this discrepancy are not included in the TDP.		communication between ASS/ASM and client applications utilizes authentication and encryption in the manner described in the web link msdn.microsoft.com/en-us/library/ms809311.aspx#dcomarch_secdis. [2009-06-01] NF: The previously stated reference is in fact included in section 2.6.2, Access Control Measures (g) in ASM TDP 2.06 System Security Specification.	Accepted: KM 6/4/2009 The web link to the encryption information is included in 2.6.2.g of the ASM TDP System Security Specification Revision 1.0, May 19, 2009.
42	1/28/09	K. Wilson	Documentation Defect	Closed	Key Card Tool 4.7.2 TDP 2.03 System Functionality Description.pdf	Key Card Tool 4.7.2 TDP 2.03 System Functionality Description.pdf refers to Premiers Windows Configuration Guide which in turn is not clear or specific about allowing or not allowing Key Card Tool to be connected to a network. Use of the wording "not intended to be used on a network" is not mandatory. As there does not appear to be a Key Card Tool Administrators guide, this information might appear in the Users Guide but cannot be found there either. (also pertinent to I:6.5.4.2 where it does not appear specifically in Premier's Client Security Policy or Gems 1.21.1 Election Administrator Guide Rev 2.0, and these are referred to in Key Card Tool 4.7.2 TDP 2.06 System Security Specification.pdf section 2.6.6)	v1: 2.2.5.3 COTS General Purpose Computer System Requirements	[2009-02-17] NF: Key Card Tool is a stand-alone application. Wording to this effect has been introduced to section 2.3.2.5.3, COTS General Purpose Computer System Requirements in Key Card Tool 4.7.2 TDP 2.03 System Functionality Description.	Accepted: GA 5/25/2009: Based on review of the delivered Key Card Tool System Functionality Description Revision 1.0, this discrepancy is closed.
43	1/28/09	K. Wilson	Documentation Defect	Closed	Key Card Tool 4.7.2 TDP 2.06 System Security Specification.pdf	Utilization of the smart cards is a security kernel and the security of the entire operation depends on the security within the smart card. Rejected: 5/27/2009 KGW -- V1: 6.2.2 "Vendors shall provide a detailed description of all system access control measures." since the vendor is reluctant to document the security of the smart cards, we will endeavor to prove they are secure. Not withstanding that, this is still a documentation discrepancy while we proceed with testing.	v1: 6.2.2.d Security kernels	[2009-02-25] NF: FEC 2002 Volume I, Subsection 6.2.2, Access Control Measures mandates the provision of examples, rather than exhaustive responses to every item listed, hence a targeted response should not have to be provided. The response to this requirement as provided in section 2.6.2, Access Control Measures in Key Card Tool 4.7.2 TDP 2.06 System Security Specification already provides examples of measures used to control access to the Key Card Tool application and data.	Rejected: KGW 5/27/2009: Accepted: KGS 6/3/2009: Documented as described. Additional security testing added to Key Card Tool tab of the Security Test Case.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
								[2009-06-01] NF: The securing of smart cards as well as the manner in which smart cards enhance application security are documented in section 5.5, Security tokens ASM TDP Appendix G: System and Data Integrity.	
44	1/28/09	K. Wilson	Documentation Defect	Closed	Key Card Tool 4.7.2 TDP 2.06 System Security Specification.pdf	Key Card Tool 4.7.2 TDP 2.06 System Security Specification.pdf states requirement is N/A. Computer Generated Password key generation is one of the purposes of Key Card Tool. Document and include any mitigation of known vulnerabilities. Rejected: 5/27/2009 KGW -- 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" I do not find a "detailed description" What devices/systems utilize the key cards generated by Key Card Tool?	v1: 6.2.2.e Computer-generated password keys	[2009-03-11] NF: Section 2.6.2, Access Control Measures (e) in Key Card Tool 4.7.2 TDP 2.06 System Security Specification has been amended to state that the Key Card Tool application is used to automatically generated the smart card and data keys. [2009-06-01] NF: Section 2.6.2, Access Control Measures (e) in Key Card Tool TDP 2.06 System Security Specification has been amended to describe the management of the integrity of Key Card Tool generated password keys as well as the manner in which these keys are used to secure ASSURE 1.2 smart card-driven products.	Rejected: KGW 5/27/2009 Accepted: KGW 6/3/2009: Sufficiently documented and any discrepancies are incorporated into #46.
45	1/28/09	K. Wilson	Documentation Defect	Closed	Key Card Tool 4.7.2 TDP 2.06 System Security Specification.pdf	Key Card Tool 4.7.2 TDP 2.06 System Security Specification.pdf states that special protocols are not used. At least one special protocol being used for access control is the ISO7816 smart card communications protocol. Rejected: 5/27/2009 KGW -- 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" Examples of "all" are provided to clarify the requirement, not to limit the "all" The statement in the TDP that Key Card Tool "not used to communicate" is incorrect. The Key Card Tool generates cards which are used to communicate keys (by physical transport) throughout the system of utilizing devices.	v1: 6.2.2.f Special protocols	[Nel, 2009-02-25] FEC 2002 Volume I, Subsection 6.2.2, Access Control Measures mandates the provision of examples, rather than exhaustive responses to every item listed, hence a targeted response should not have to be provided. The response to this requirement as provided in section 2.6.2, Access Control Measures in Key Card Tool 4.7.2 TDP 2.06 System Security Specification already provides examples of measures used to control access to the Key Card Tool application and data.	Rejected: KGW 5/27/2009 Accepted: GA 6/18/2009: Review of Section 2.6.2 of the Key Card Tool TDP System Security Specification Revision 2.0 dated 17 June 2009 verifies that the special protocol is provided within the TDP.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
46	1/28/09	K. Wilson	Documentation Defect	Closed	Key Card Tool 4.7.2 TDP 2.06 System Security Specification.pdf	Key Card Tool 4.7.2 TDP 2.06 System Security Specification.pdf states that message encryption is N/A. Key Card Tool generates a key. What is this key used for if not encryption? If it is not encryption it is some other access control protocol that needs to be documented since the section header states "all system access control measures ... such as." Other protocols that this reviewer found by easily traversing some of the code includes AES, Diffie-Hellman, MD5, HMAC-MD5, DES, SHA1, and RSA (signatures and key exchange). Rejected: 5/27/2009 KGW -- 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" Examples of "all" are provided to clarify the requirement, not to limit it. Still missing references to what devices Key Card Tool generates keys for and references to how these keys are used. Where if not here is the bit-strength and encryption algorithm documented? Where if not here is the entropy of the random-number key generation documented? Rejected: 6/3/2009 KGW -- Key Card Tool 4.7.2 User's Guide section 2 does not provide the following information: a) What file(s) on the Voter Access Card, Supervisor Card and Central Administrator card are encrypted with the key generated by Key Card Tool b) section 2.2.2 states that "data keys are used ... to digitally sign election data" We understand the Key Card Tool generates a symmetric encryption key. Does it also generate public/private key pairs for digital signature generation?	v1: 6.2.2.g Message encryption and	[2009-02-24] NF: FEC 2002 Volume I, Subsection 6.2.2, Access Control Measures mandates the provision of examples, rather than exhaustive responses to every item listed, hence a targeted response should not have to be provided. The response to this requirement as provided in section 2.6.2, Access Control Measures in Key Card Tool 4.7.2 TDP 2.06 System Security Specification already provides examples of measures used to control access to the Key Card Tool application and data. [2009-06-02] NF: The devices that Key Card Tool generates keys for and references to how these keys are used are documented in section 2, Concepts in the Key Card Tool User's Guide (this reference is included in section 2.6.2, Access Control Measures (e) in ASM TDP 2.06 System Security Specification).	Rejected KGW 5/27/2009 Rejected KGW 6/3/2009 Accepted: SJ 6/26/2009: Updated Key Card Tool documentation referencing AVOSX,TSX and TS (Encryption algorithm is documented).

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						c) section 2.2.2 "Data keys are used to encrypt election results" What electrically transmitted file(s) are encrypted utilizing this key, especially any files that can be transmitted by telephony. If this is the case, please explain how GEMS has access to this key since it does not seem to require a smart-card reader connection. Or does this statement only refer to the election results residing on the memory cards of the TS-R6, TSX, and OSX? In that case please list those file or file types so encrypted. d) this section does not document the algorithm or bit-strength of the key. Did not find that information in the "FEC 2002 Key Card Tool Technical Data Package System Security Specification" dated May 2009			
47	1/28/09	K. Wilson	Documentation Defect	Closed	Key Card Tool 4.7.2 TDP 2.06 System Security Specification.pdf	Key Card Tool 4.7.2 TDP 2.06 System Security Specification.pdf does not address this requirement.	v1: 6.4.2 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.	[2009-02-23] NF: The specified requirement is addressed in section 2.6.8.2, Protection Against Malicious Software in Key Card Tool 4.7.2 TDP 2.06 System Security Specification.	Accepted: KGW 5/27/2009 Closed
48	1/28/09	K. Wilson	Documentation Defect	Closed	PCS TDP	PCS 2.2.1 TDP 2.03 System Functionality Description.pdf states the OS is "NT or equivalent." Specific operating systems, version and service packs must be declared as part of the tested system. Also cannot find this information in PCS 2.2.1 TDP 2.08 System Operations Procedures.pdf or PCS 2.2.1 TDP 2.04 System Hardware Specification.pdf	v1: 2.2.5.3 COTS General Purpose Computer System Requirements	[2009-02-17] NF: Section 2.3.2.5.3, COTS General Purpose Computer System Requirements in PCS 2.2.1 TDP 2.03 System Functionality Description has been amended to state that PCS runs on the Windows XP operating system.	Accepted: GA 7/6/2009: Review of the PCS 2.2.1 TDP 2.03 System Functionality Description Revision 1.0 dated 21 May 2009 validates that the references to the NT Operating System are deleted.
49	1/28/09	K. Wilson	Documentation Defect	Closed	PCS TDP	Unable to find any documentation stating a "description of recommended policies for" access control of PCS roles/duties such as Administrator, Supervisor, Security Administrator, Scanner technician,	v1:6.2.1 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 a)	[2009-02-23] NF: Software access control policy relevant to the use of the PCS application, expressed in terms of the roles involved in the use of the application, the duties associated with these roles, and	Accepted: GA 5/25/2009: Based on review of the updated TDP, this discrepancy is closed.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						Adjudicator.	Software access controls etc.	the qualifications associated with each role is documented in section 12, Election Personnel in the GEMS_Election_Administrators_Guide_1.21.3_or_later_Rev_1.0.	
50	1/28/09	K. Wilson	Documentation Defect	Closed	PCS 2.2.1 TDP 2.06 System Security Specifications.pdf	PCS 2.2.1 TDP 2.06 System Security Specifications.pdf does not address this set of requirements. Since PCS is specifically designed to handle ballots, ballot counting, counting operations and reporting data in a central count location, these requirements must be addressed.	v1: 6.3.2 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	[Nel, 2009-02-25] Section 2.6.7.2, Central Count Location Security in PCS 2.2.1 TDP 2.06 System Security Specifications now includes a reference to section 8, Absentee Ballot Processing in the GEMS_Election_Administrators_Guide_1.21.3_or_later_Rev_1.0, which provides the required information.	Accepted: KM 6/12/2009 KM: The reference to the GEMS document is now provided in the PCS TDP 2.06.
51	1/28/09	K. Wilson	Documentation Defect	Closed	GEMS 1.21.1 TDP 2.06 System Security Specifications.pdf	GEMS 1.21.1 TDP 2.06 System Security Specifications.pdf does not address I:6.4.2. System utilizes public telecommunications systems so this requirement is applicable. Rejected: 5/25/09 GA: The references in the GEMS 1.21.1 TDP 2.06 System Security Specifications address initial system configuration and not the procedure to be followed to ensure that such protections is maintained.	v1: 6.4.2 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.	[2009-02-17] NF: A response has in fact been provided to this requirement in section 2.6.8.2, Protection Against Malicious Software in GEMS 1.21.1 TDP 2.06 System Security Specifications. [2009-06-01] NF: Sections 7, Physical Security Practices and 8, Network Security Practice in Premier's Client Security Policy referenced in section 2.6.8.2, Protection Against Malicious Software in GEMS TDP 2.06 System Security Specifications do in fact represent security policy to remain in effect throughout the election process, and not just at the point of initial system configuration. Section 2.6.8.2, Protection Against Malicious Software in GEMS TDP 2.06 System Security Specifications has been amended to include a description of the manner in which the relevant security policy, procedures, and functionality are maintained current by way of reference to section 2.6.5.4.3, Monitoring and Responding to External Threats in the same document.	Rejected: GA 5/25/2009 Accepted: DEV 06/19/2009: Verified the addition of section 3.2.1 of Premiers Windows Configuration Guide Rev 10.0 and FEC 2002 GEMS Technical Data Package System Security Specification Revision 2.0 June 17, 2009 sections 2.6.5 and 2.6.5.4.3.
52	1/28/09	K. Wilson	Documentation Defect	Closed	GEMS TDP	Unable to find where II:6.4.2.a-g are addressed for GEMS and/or voting devices that utilize telecommunications	v1: 6.4.2.a Identification of new threats and their impact	[Nel, 2009-02-17] The requirements specified in Volume II, Subsection 6.4.2, Data Interception and Disruption are	Accepted: GA 5/25/2009: Documentation referenced in the

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
								addressed in section 2.6.5.4.3, Monitoring and Responding to External Threats in GEMS 1.21.1 TDP 2.06 System Security Specifications. Note that the wrong volume of the 2002 FEC is referenced - volume I as opposed to volume II.	vendor response is sufficient and this discrepancy is closed.
53	8/22/08	SysTest (#22 on Discrepancy Report Ballot Station Rev 08.xls)	Documentation Defect	Closed	BallotStation 4.7.3 System Administrators Guide, Rev 1.0, 06/25/08 BallotStation 4.7.3 Users Guide, Rev 2.0, 07/09/08	The documentation does not have any reference to the error message when a memory card has reached its maximum capacity for data storage, for the Ballot Station application. The discrepancy remains open because the vendor's error messages still do not address.	VSS Vol.2; 2.8.5.b The vendor shall provide documentation of system operating procedures that meet the following requirements: b. Provides procedures that clearly enable the operator to access the control flow of system functions (as evidenced by system	Discrepancy resolved in BallotStation User's Guide Rev. 3.0, Appendix F: Error and Failure Recovery.	Accepted: GA 3/18/2009: Review of document referenced.
54	8/22/08	SysTest (#12 on Discrepancy Report PCS Rev 04 Premier 020908.xls)	Documentation Defect	Closed	PCS 2.2.1 Users Guide, Rev 1.0, 06/23/08 PCS 2.2.1 System Administrators Guide, Rev 1.0, 06/24/08	The documentation does not specify when and/or how the message that discribes an 'out-of-date' workspace will appear, or how its generated in the PCS application.	VSS Vol.2; 2.8.5.b The vendor shall provide documentation of system operating procedures that meet the following requirements: b. Provides procedures that clearly enable the operator to access the control flow of system functions (as evidenced by system	See section 5.1, Workspace screen in the PCS 2.2.1 User's Guide Revision 2.0. The lower frame of the PCS interface reports the status of the scanner(s), displays information relating to the active workspace, and reports the status of decks processed for	Accepted: GA 3/18/2009: Review of document referenced.
55	1/30/09	K. Wilson	Documentation Defect	Closed	TS R6 TDP	While there are no specific requirements for wireless transmissions in the VSS, such transmission is covered by other telecommunications requirements as stated in I:5.1.1. The TSX units have IrDA ports, and there needs to be documentation covering these transmissions. Rejected: 5/25/09 GA: Updated to reflect TS R6 not TSX. Review of the Window CE 3.0 Build Process revision 5.0 lists the WinCE 3.0 operating system software that is compiled and linked and the Build Configuration Guide revision 15 Section 3.2 but on the MSDN site, the Windows CE 3.0 enhancements include support drivers for IrDA and	vol2:2.4 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.	[2009-03-17] NF: The AccuVote-TSX does not have an IrDA port, but the AccuVote-TS R6 does. BallotStation does not make any use of the IrDA port. No drivers are installed in Windows CE 3.0 to support the use of the IrDa port. [2009-06-02] NF: The wireless drivers referenced are not included in the applicable Windows CE 3.0 build. [2009-06-09, Tab] The AccuVote-TS R6 does not use the Infrared driver. See the "AccuVoteTS/_PUBLIC/ACCUVOTETS_IDE/WINCE300/Oak/Misc/cesysgen.bat" file line 57 "REM ***** not used -> set CE_MODULES=%CE_MODULES	Rejected: GA 5/25/2009 Accepted: KM 6/12/2009: The "AccuVoteTS/_PUBLIC/ACCUVOTETS_IDE/WINCE300/Oak/Misc/cesysgen.bat" command to include the IR driver has been marked as a comment, so the driver file is not copied into WinCE during the build process.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						the IrDA protocol.		% ircomm irdastk"	
56	1/30/09	K. Wilson	Documentation Defect	Closed	Assure 1.2 TDP	The TDP does not contain a detailed overview of communications related to telecommunications and the use of public networks to address this VSS requirement. In so far as any networking capability might relate to a telecommunications capability, a detailed overview of all networking in its broadest sense needs to be submitted for certification. Rejected: 5/27/2009 KGW -- V2: 2.2"In the system overview, the vendor shall provide information that enables the test authority to identify the functional and physical components of the system, how the components are structured, and the interfaces between them" Then in V2:2.4 "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" Where is the system overview that contains this information? Perhaps I missed it. Vendor review of the IBeta telecommunications diagram will help close this discrepancy as it will show that at least we understand the system.	vol2:2.4 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.	[2009-03-04] NF: The discrepancy reported requests a detailed overview of telecommunications functionality and public network use, but this is not what the referenced requirement states. COTS telecommunications used by ASSURE 1.2 products are documented in ASSURE 1.2 TDP Appendix 1: COTS Communication Components in the ASSURE 1.2 TDP Documents. Detailed specifications of the hardware components of ASSURE 1.2 voting devices, including specifications of hardware used to support the telecommunications capabilities of the system are provided in the following TDPs: AccuVote-OS: AccuVote-OS TDP Appendix A: Hardware Specifications, AccuVote-OS TDP Appendix B: Drawings, AccuVote-OS TDP Appendix C: COTS Component Specifications, AccuVote-OS TDP Appendix E: AccuFeed Specifications AccuVote-OSX: AccuVote-OSX TDP Appendix B: Hardware Specifications, AccuVote-OSX TDP Appendix C: Drawings, AccuVote-OSX TDP Appendix D: COTS Component Specifications AccuVote-TS R6: AccuVote-TS R6 TDP Appendix B: Hardware Specifications, AccuVote-TS R6 TDP Appendix C: Drawings, AccuVote-TS R6 TDP Appendix D: COTS Component Specifications, AccuVote-TS R6 TDP Appendix E: VIBS Keypad Specification AccuVote-TSX: AccuVote-TSX with AVPM TDP Appendix B: Hardware Specifications, AccuVote-TSX with AVPM TDP Appendix C: Drawings, AccuVote-TSX with AVPM TDP Appendix D: COTS Component Specifications, AccuVote-TSX with AVPM TDP Appendix E: VIBS Keypad Specification.	Rejected: KGW 5/27/2009 Accepted: GA 7/6/2009: Based on Premier's response that the diagram that iBeta created from the Premier TDP does represent the voting system telecommunications and use of public networks, this verifies that the TDP meets the TDP requirements to allow the VSTL to adequately test the voting system and this discrepancy is closed.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
								[2009-06-11] NF: The diagram does provide an appropriate representation of the ASSURE 1.2 system.	
57	1/30/09	K. Wilson	Documentation Defect	Closed	OS-PC AccuVote-OS Precinct Count 1.96.11 TDP 2.14 Telecommunications.pdf OSx: AccuVote-OSX 1.2.1 TDP 2.14 Telecommunications.pdf TS, TSx: BallotStation 4.7.3 TDP 2.14 Telecommunications.pdf, AccuVote-TSX with AVPM TDP 2.14 Telecommunications.pdf	Numerous documents claim that the system does not utilize a WAN. OS-PC AccuVote-OS Precinct Count 1.96.11 TDP 2.14 Telecommunications.pdf OSx: AccuVote-OSX 1.2.1 TDP 2.14 Telecommunications.pdf TS, TSx: BallotStation 4.7.3 TDP 2.14 Telecommunications.pdf, AccuVote-TSX with AVPM TDP 2.14 Telecommunications.pdf Vendor needs to provide further explanations as to why the use of a modem to transport information over public telephone systems is not within the given definition within the VSS requirement.	vol1:5.1 A wide area network (WAN) public telecommunications component consists of the hardware and software to transport information, over shared, public (i.e., commercial or governmental) circuitry, or among private systems. ... vol1:5.2.6 For WANs using public telecommunications, boundary definition and implementation shall meet the following requirements. [a) ... b) ..., c) ....]	[2009-06-10] TI: TDP's have been updated to correctly include information about the WAN usage.	Accepted: SS 06/16/2009: Based on review of the updated TDP, this discrepancy is closed.
58	2/23/09	S. Jakileti	Documentation Defect	Closed	AccuView Printer Module 3.0 Build Process Configuration Guide Rev 16	A number of COTS programs listed in the documentation can no longer be acquired directly from the manufacturers.	v2; 2.5.3 :The vendor shall also include a certification that procured software items were obtained directly from the manufacturer or a licensed dealer or distributor.	Certification of Procured Software Letter provided on 26 February 2009.	Accepted: GA 2/27/2009: Receipt and review of letter confirmed the applications are COTS.
59	2/23/09	L. Laboe	Documentation Defect	Closed	Windows CE 4.10 Build Process Revision 5.0 September 30, 2008	AVValidator.XML file is not being loaded as part of the build and installation process in the WinCE4.10 Build Process.	v2; 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	[2009-05-25] WL: Revised description in Windows CE 3.0 Build Process Revision 6.0 Sec. 3, Windows CE 4.1 Build Process Revision 6.0 Sec.3, Windows CE 5.0 Build Process Revision 9.0 Sec. 3. [2009-06-10] NF: The Windows CE 4.1 build process has been updated to include AVValidator.xml as build output. This build process is reflected in AccuVote-TSX with AVPM TDP Appendix K: Windows CE Build Process in the updated	Accepted: DEV 06/19/2008: Verified Section 3 of AccuVote-TSX with AVPM Appendix K (Rev 6.0 there is not a Rev 9.0) states AVValidator.XML is loaded as part of the build WinCE build process.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
								AccuVoteTSX with AVPM TDP.	
60	2/23/09	L. Laboe	Documentation Defect	Closed	Windows CE 4.10 Build Process Revision 5.0 September 30, 2008 Windows CE 3.0 Build Process Revision 5.0 September 30, 2008 WinCE 5.0 Build Process Revision 8.0 September 30, 2008	No mention where to place the makeavinstall.exe file. During the trusted build, iBeta placed this in the release directory per witness instruction.	v2; 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	[2009-05-06] WL: The path to copied to is listed in Windows CE 3.0 Build Process Revision 5.0 Sec. 3, Windows CE 4.1 Build Process Revision 5.0 Sec. 3, Windows CE 5.0 Build Process Revision 8.0 Sec. 3.	Accepted: DEV 06/19/2008: Verified Section 3 of AccuVote-TSX with AVPM Appendix K (Rev 6.0 there is not a Rev 8.0) states copy the cited file into the C:\WINDOWS\system32\ folder.
61	3/18/09	K. Wilson	Documentation Defect	Closed	AutoMARK Premier VAT Software and Firmware Compilation Instructions Rev 9	The document does not contain a procedure to upgrade the PEB firmware on the A100 model, but the A100 model is included in the Premier application.	v1: 4.1.1 the vendors shall submit to the ITA, in the TDP, a record of all user selections made during software installation.	[2009-05-19] PH: Procedure added to rev. 12 of the AutoMARK VAT Software and Firmware Compilation Instructions AQS-13-5013-000-A.doc dated 5/8/2009. This document was checked in during the trusted build. Section added: 4.8.e	Accepted: GA 5/25/2009: Receipt, review, and use of the updated documentation closes this discrepancy.
62	3/18/09	K. Wilson	Documentation Defect	Closed	TDP - AVOS Documentation	No documentation for the COTS modem used in AVOS-PC Model A. Found corresponding modem for Model C in Multitech_EmbeddedDataModems.pdf.	v1: 6.5.4.1.c 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 ... modems	[2009-05-19] NF: A specification sheet for the AccuVote-OS model A modem is now provided in the folder Models A & B in the folder Modem in AccuVote-OS TDP Appendix C: COTS Component Specifications in AccuVote-OS TDP Revision 5.0.	Accepted: GA 5/25/2009: Receipt and review of the updated documentation closes this discrepancy.
63	4/21/09	C.Cvetezar	Informational	Closed	GEMS 1.21.1 Reference Guide Rev 3.0, Section 2.3. List view tabs GEMS->Default Precincts->Report Precinct GEMS->Individual Precinct->Vote Center GEMS->Individual Race->Vote	Header discrepancies between GEMS 1.21.2 software and documentation: a) ICON = Default precincts, TAB = Report Precinct: documentation shows Method in FIELD LABEL whereas the software displays Catagory for this heading. b) ICON = Individual Precinct, TAB = Vote Center: documentation shows MCVers in FIELD LABEL whereas the software displays MC Ver for this heading. b) ICON = Individual Race, TAB = Vote Center: documentation shows MCVers in FIELD LABEL whereas the software displays MC Ver for this heading.		[20-05-09] TT: Informational deficiency addressed in GEMS Reference Guide 1.21.3 or later Rev 2.0.	Accepted: SS 6/17/2009: Based on review of the updated TDP, this discrepancy is closed.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
					Center				
64	4/21/09	C.Cvetezar	Functional Defect	Closed	GEMS 1.21.2 text editing fonts (Setup->Voter Groups…, Setup->Race Options…,etc.)	Default font presented in drop-downs for font editing is "Arial Narrow". If this font does not exist on the system, no warnings are given and some font (Arial) was automatically chosen instead.	2.3.1.2b: All systems shall provide a capability for: b. Rapid and error-free definition of elections and their associated ballot layouts;	[2009-05-06] SL: This is a standard Windows's behavior. Obviously, at one time, the font was there. If the font is no longer available, font substitution will take place. Microsoft's Wordpad does exactly the same thing. Font substitution does not constitute an error in ballot layouts.	Accepted: CAC 5/25/2009: Vendor response is sufficient and this discrepancy is closed.
65	4/21/09	C.Cvetezar	Documentation Defect	Closed	GEMS 1.21.1 User's Guide Revision 3.0, Section 3.8.2. Margins	Document does not have any reference that explains the "Force Re-Layout" check box.	v1: 7.7a: 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…	[2009-05-20] TT: Added Force Re-Layout option description in section 3.8.2, Margins, in the GEMS User Guide 1.21.3 or later Rev 3.0.	Accepted: KM 6/10/2009: GEMS_Users_Guide_1.21.3_or_later_Rev_3.0 has been updated with information about "Force Re-Layout."
66	4/21/09	C.Cvetezar	Documentation Defect	Closed	PCS_2.2.1_Users_Guide_Rev_1.0, Section 3.9.7. Rules Profile	Document does not have any reference that explains the Load Profile, Save Profile and Reset buttons in any detail.	v1: 7.7a: 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…	[2009-05-20] TT: Revised description in section 3.9.7 Rules Profile in the PCS User's Guide 2.2.2 or later Rev 3.0.	Accepted: KM 6/10/2009: PCS_Users_Guide_2.2.2_or_later_Rev_3.0, section 3.9.7, has been updated with descriptions of the Load Profile, Save Profile and Reset buttons.
67	4/21/09	K. Mathis	Functional Defect	Closed	TSX Model A Affects both models (AVPM and non-AVPM)	With + or - 4Kv contact on the headphone jack during ESD testing caused the TSX to stop playing sound and lock up after the voter chooses to cast their ballot. The ballot was not cast before the unit hangs.	IEC 61000-4-2 (1995-01) and vol.1 sect. VSS 3.2.2.8./VVSG 4.1.2.8 Verify vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand ±15 kV air discharge and ±8 kV contact discharge without damage or loss of data.	[2009-05-19] KL: After reviewing the problem, EC#AD586 was issued to introduce a TSX model A & B model upgrade kit. This kit includes 3 varistors and a copper grounding pad that are added to the motherboard. Subsequent testing by iBeta demonstrated the fix was effective.	Accepted: KM 6/2/2009: This issue is addressed by EC#AD586.
68	4/21/09	K. Mathis	Functional Defect	Closed	TSX Models A, C, and D	Contacting the top seam of the TSX tablet with -15Kv Air during ESD testing will disable the TSX motherboard.	IEC 61000-4-2 (1995-01) and vol.1 sect. VSS 3.2.2.8./VVSG 4.1.2.8 Verify vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand ±15 kV air discharge and ±8 kV contact discharge without damage or loss of data.	[2009-05-19] KL: After reviewing the problem, EC#AD586 was issued to revise the TSX upgrade kits. The change to the kit is replacing the inverter insulator with a longer version that covers the length of the motherboard.. Subsequent testing by iBeta demonstrated the fix was effective.	Accepted: KM 6/2/2009: This issue is addressed by EC#AD586.
69	4/21/09	K. Mathis	Functional Defect	Closed	AVPM TSX Stand	Contacting the right side of the AVPM housing (near the internal metal bracket) with -15Kv Air during ESD testing disrupted the communications between the TSX	IEC 61000-4-2 (1995-01) and vol.1 sect. VSS 3.2.2.8./VVSG 4.1.2.8 Verify vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able	[2009-05-19] KL: After reviewing the problem, EC#AD586 was issued to revise the TSX upgrade kits. The kit adds a longer screw to replace the one mounting the	Accepted: KM 6/2/2009: This issue is addressed by EC#AD586.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						and the AVPM printer. Contacting the Horizontal Coupling Plane with + or -8Kv during ESD testing disrupted communications between the TSX and the AVPM printer. This error cannot be recovered without rebooting the TSX.	to withstand ±15 kV air discharge and ±8 kV contact discharge without damage or loss of data.	leg clip. This longer screw grounds the leg assembly to the power supply housing. Subsequent testing by iBeta demonstrated the fix was effective.	
70	4/21/09	K. Mathis	Functional Defect	Closed	VIBS Keypad	Contacting the VIBS keypad during ESD testing with + or -15Kv air near any of the buttons disables the circuit board in the keypad.	IEC 61000-4-2 (1995-01) and vol.1 sect. VSS 3.2.2.8./VVSG 4.1.2.8 Verify vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand ±15 kV air discharge and ±8 kV contact discharge without damage or loss of data.	[2009-05-19] KL: After reviewing the problem, EC#AD586 was issued to introduce a VIBS keypad upgrade kit. The kit includes two insulators, one between the circuit card and elastomer pad and the other along the top edge of the circuit card. Subsequent testing by iBeta demonstrated the fix was effective.	Accepted: KM 6/2/2009: This issue is addressed by EC#AD586.
71	4/21/09	C.Cvetezar	Documentation Defect	Closed	GEMS 1.21.1 User's Guide Revision 3.0, Section 7.2. Importing audio	Document does not have any reference that explains: a) Format button b) Default button	v1: 7.7a: 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…	[20-05-09] TT: Revised description in section 7.2 Importing Audio in the GEMS User's Guide 1.21.3 or later Rev 3.0.	Accepted: KM 6/11/2009: GEMS_Reference_Guide_1.21.3_or_later_Rev_2.0 contains information on the Format and Default buttons.
72	4/21/09	C.Cvetezar	Documentation Defect	Closed	GEMS 1.21.1 User's Guide Revision 3.0, Section 7.1. Recording audio	Document does not have any reference that explains the TTS button.	v1: 7.7a: 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…		Accepted: GA 5/25/2009: Closed as a duplicate of Discrepancy #80.
73	4/23/09	C.Cvetezar	Functional Defect	Closed	GEMS->Generate Ballots	1) Spreadsheet: GEN02 System Test Case Assure 1.2.xls Database: GEN02_PaperColorError9-04240913.gbf Error Screenshot: Util.h error GEMS.jpg provided to Premier via email on 5/8/09. In Race Options, setting the Group candidates by Vgroup on races in this database and then Generate Ballots causes the error as shown in the enclosed screenshot resulting in the ballots not being generated. In this case the Group candidates by Vgroup was checked for the	1) v2: 5.4.2p: … All messages shall be self-explanatory and shall not require the operator to perform any look-up to interpret them, except for error messages that require resolution by a trained technician. 2) v2:2.5.6.2d: The vendor shall describe the software's capabilities or methods for detecting or handling: ... Error logging for audit record generation;	[25-05-09] TT: Revised description in Appendix D, Error Messages in the GEMS Reference Guide 1.21.3 or later Rev 2.0. [2009-06-10] RP: BUG#10142 to be fixed in GEMS 1.21.3.1	Accepted: CAC 06/30/2009: Closed - Validated during GEN02-R regression testing of GEMS 1.21.4

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						following races: President Straight Party Election Judges Prop 18 (which I did not mean to set but did anyway) State Assembly District 1 State Assembly District 2 If no error was present, the tester would then start setting Group candidates by Vgroup in other partisan races. 2) GEMS Audit Log does NOT log this error			
74	4/18/09	J. Patterson	Functional Defect	Closed	All equipment tested	None of the equipment supplied for testing contain a service data plate. No service or preventative maintenance schedule or list of operation was found on or in the unit. 6/23/09 GA: The Service Label provided in an email for the AVOSX provides the data plate required data per the requirement. An EC for all the equipment is required.	3.4.6 b Each device shall display a separate data plate containing a schedule for and list of operations required to service or to perform preventive maintenance	[2009-06-24] KRL: Engineering change AD813 will release the service labels for the AccuFeed, AVTS, AVTSX, AVOS, AVOS Ballot Box, AVOSX and AVOSX Ballot box. These labels will be added to the field upgrade kits initially released under EC#A2322.	Accepted: JP 6/30/2009: EC#AD813 Includes the remaining equipment, and the Service Label does provide the information required.
75	5/9/09	C.Cvetezar	Functional Defect	Closed	Election race display on the AutoMARK 300 running PVR/PAVR 3342.	In GEN02 test execution (straight party, General Election), 4 voter groups were assigned to the Straight Party race (REP, DEM, PRO, KN). This election also had cross-endorsed candidates for State Election Judges and State Assembly. When SP REP is selected, both State Election Judges and State Assembly races are presented to the voter; however, when either DEM, PRO or KN is selected for SP, only the State Assembly race is presented to the voter. Supporting files: on CF card (election data for AutoMARK).	2.3.1.2 b Ballot formatting is the process by which election officials or their designees use election databases…. All systems shall provide a capability for: rapid and error-free definition of elections and their associated ballot layouts.		Accepted: CAC 05/20/2009: It was determined that tester error in linking the State Election Judges to Republican instead of <NP> was the cause of this error.
76	5/9/09	C.Cvetezar	Documentation Defect	Closed	Ballot marking on the AutoMARK 300 running PVR/PAVR 3342.	In GEN02 test execution (straight party, General Election), voter 24 voted blank straight party race, President - KN, State Election Judges: Hansen (KN), Labonte (KN), Gordon (REP). Summay of	V1: 2.2.1.a To ensure vote accuracy, all systems shall: a. Record the election contests, candidates, and issues exactly as defined by election officials;	[2009-05-20] TT: See Appendix B, AutoMARK VAT Considerations in the GEMS User's Guide 1.21.3 or later Rev 3.0. This appendix describes considerations that must be observed when defining ballots	Rejected: DEV 05/11/2009 Accepted: CAC 6/01/2009: Vender's response

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						Selections display was correct; however, ballot marked State Election Judges: Yackie (PRO), Smith (PRO) and a Write-In. Supporting files on SharePoint GEN02 Discrepancy screenshots: AutoMARK Summary of Selections 1of4.JPG through AutoMARK Summary of Selections 4of4.JPG. Other supporting files: on CF card (election data for AutoMARK). Rejected: 05/11/09 DEV - Discussed issue with client and it was determined the failure was due to the write-ins being placed at the beginning of the races. AIMS only recognizes write-ins if they are listed at the end. Verified the AutoMARK PREM Poll Workers Guide, dated 02/11/08 provides examples of different races/candidates, but does state the write-ins must be located at the end of the race in order for correct ballot marking.		for use on AutoMARK VAT devices. It includes a note that states that write-in candidate names must be placed at the very end of the race's candidate list.	accepted; GEMS User's Guide, Appendix B states that the write-in candidate names must appear at the very end of the candidate list.
77	5/9/09	C.Cvetezar	Documentation Defect	Closed	Assure Security Manager/Service logins.	The first login screen for ASM must be ASSURE_USER; this is not documented in the TDP. The second login screen for ASS is not documented in the TDP.	v1: 7.7a: 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…	[2009-05-20] TT: Reviewer is incorrect. First login for ASM is not performed by ASSURE_USER. There is no first or 'second login screen for ASS'. ASM login procedures are correctly documented in the ASSURE Security Manager Users Guide 1.2.2_or_later_Rev_2.0.	Accepted: CAC 5/25/2009: Vendor response is sufficient and this discrepancy is closed due to tester error.
78	5/9/09	C.Cvetezar	Functional Defect or Documentation Defect	Closed	AccuVote-OS Precinct Count User's Guide 1.96.11 or later: 7.3. Counting test ballots: 6. RECIRCULATE BALLOTS?	Selecting YES to RECIRCULATE BALLOTS? Prompt only returns the inserted ballot. TDP documentation does not address this mode. Rejected: 06-01-09 CAC: TDP documentation only address the NO selection to RECIRCULATE BALLOTS? question not the YES. Without documentation as an expected result, the requirement is not met. Rejected: 06-09-09 KM: The documentation does not provide information for the user as to what pressing "YES" does - where is it	v1: 7.7a: 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…	[2009-06-19] TT: Pressing YES to the Re-circulate ballots? prompt is documented in section 14.11.4, Re-circulating ballots, in the AccuVote-OS Precinct Count User's Guide 1.96.11 or later, Rev 1.0. The referenced document has been delivered.	Rejected: CAC 06/01/2009 Rejected: KM 06/09/2009 Accepted: CAC 06/24/2009: AccuVote-OS Precinct Count User's Guide 1.96.11 or later v1.0 is sufficient and this discrepancy is closed.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						documented that pressing yes for "Recirculate ballots" does. The Premier response is that it does what it is expected to do but the documentation does not support that response.			
79	5/9/09	C.Cvetezar	Functional Defect	Closed	BallotStaion 4.7.5, AccuVote TSX: Cast Ballot confirmation	On the TSX running BallotStation 4.7.5 the Cast Ballot confirmation screen displays the correct precinct and increments the vote count; however, the screen always displays POLPARTY no matter what voter group was chosen in straight party race. The AVPM printout also shows the same information. Related: the 4th vote displayed POLPARTY 3 on the screen but the AVPM printout displayed POLPARTY 4. Supporting files on SharePoint GEN02 Discrepancy screenshots: BallotStation4.7.5 - POLPARTY 1 of 2.JPG and BallotStation4.7.5 - POLPARTY 2 of 2.JPG	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-05-25] IG: GEN02_ElectionInstallASM_0905051406.gbf' database for that issue is not correctly defined. The 'State Election Judges' race is assigned to 'Republican' voter group (see Race Options> Voter Group 1). This is the way to define Primary election, not a General election. If you assign NP as a 'Voter Group 1' for that race, the confirmation screen in BS won't show any party references.	Accepted: CAC 5/25/2009: Vendor response is sufficient and this discrepancy is closed.
80	5/19/09	D. Valdez	Documentation Defect	Closed	GEMS User's Guide 1.21.3 or later, Revision 2.0, April 16, 2009; GEMS Reference Guide 1.21.3 or later, Revision 1.0, April 20, 2009	The TDP documentation does not discuss the "Text to Speech" option available in GEMS.	v1: 7.7a: 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…	[2009-05-25] TT: Revised description in section 7.1 Recording Audio in the GEMS User's Guide 1.21.3 or later Rev 3.0.	Accepted: KM 6/11/2009: GEMS_Reference_Guide_1.21.3_or_later_Rev_2.0 tells the user to look in their Windows documentation for information on Microsoft's TTS feature.
81	5/19/09	D. Valdez	Documentation Defect	Closed	GEMS User's Guide 1.21.3 or later, Revision 2.0, April 16, 2009; GEMS Reference Guide 1.21.3 or later, Revision 1.0, April 20, 2010	The TDP documentation does not mention that the audio option is not selectable for write-in candidates.	v1: 7.7a: 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…	[2009-05-25] TT: Revised description in section 7, Audio in the GEMS User's Guide 1.21.3 or later Rev 3.0.	Accepted: KM 6/11/2009: GEMS_Reference_Guide_1.21.3_or_later_Rev_2.0 tells the header for section 7 makes note that no audio need be recorded for write-in candidates.
82	5/19/09	D. Valdez	Documentation Defect	Closed	AutoMARK PREM Poll Worker's Guide	GEMS was coded with a ballot containing both English and Chinese. The dual language ballot did not appear on the VAT. Only the	v1: 7.7a: Vendors are required to produce documentation to support the development and formal testing of voting systems…a. Be sufficient to	[2009-05-25] IG: It works as expected. The behavior is the same as in Ballot Station. When you select the Language under the	Accepted: CAC 5/26/2009: Vendor response is sufficient and this

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
					Revision 6 February 11, 2008; AIMS PREM Sect05 Election Officials Guide Rev 12 February 21, 2008	language selected appeared. The TDP documentation does not state whether or not dual language ballots are supported.	serve the needs of the ITA…	'Language Selection' screen, the upcoming ballot is getting displayed in corresponding language. There is no way to present a ballot in multi languages in the same time	discrepancy is closed.
83	5/19/09	D. Valdez	Functional Defect	Closed	BallotStation (TSX and R6)	During GEN03 testing, a Chinese ballot was left on the screen for approximately 10 minutes (s/b 2.5 minutes) and the ballot time-out prompts never appeared and the ballot(s) could not be cancelled. A hard re-boot had to be performed to turn the units off since the Voter Access Card could not be removed. Rejected: 05-25-2009 CAC: We are using VIBS. non-VIBS ballot time-out does work fine. BallotStation Users Guide states: 5.3. Ballot time-out and ballot cancellations In Election Mode each ballot display screen pauses for 150 seconds, to allow the voter to make his or her selections. If the voter does not provide input of any kind for 150 seconds, a warning prompt alerts the voter that unless the voter touches the "Resume" button within 30 seconds, the ballot will be cancelled. The warning prompt is followed by a countdown message appears along with a large, obvious "Resume" button at the bottom of the display. If the voter touches the Resume button, he or she is returned to the ballot. If the Resume button is not touched, the ballot is cancelled. If the ballot is cancelled, the voter is prompted to remove the voter access card and seek the assistance of a pollworker. Rejected: 06-01-2009 CAC: In this section, there is no distinction between VIBS and non-VIBS mode. Since GEN03 is an audio election, we use VIBS (or	V1: 2.2.7.2.3):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; V1: 2.2.7.2.3):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; HAVA 2002: 301.3.a: ...in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters;	[2009-05-25] IG: Please make sure you are using the 'Ballot Time-Out' feature in Election Mode and non-VIBS ballot ONLY. It is not supported under the Pre-Election Mode and VIBS ballot(s). [2009-05-29] TT: Discrepancy is invalid; feature works as expected for visual ballots. Added description of how to cancel an Audio Ballot (Hidden or non-Hidden) to the BallotStation Users Guide 4.7.5 or later Rev 2.0, and to the AccuVote-TSX Pollworkers Guide Rev 12.0. [2009-06-19] TT: The reviewer is correct. The unit does not time out after 150 seconds of inactivity is detected when voting a Hidden or non-Hidden Audio ballot. If a voter voting a Hidden or non-Hidden Audio ballot flees or leaves, the ballot must be cancelled by a pollworker. To clarify the expected behavior, I have added the previous two lines of text to the BallotStation User's Guide 4.7.5 or later Rev 3.0, to the AccuVote-TS R6 Pollworker's Guide Rev. 7.0 and to the AccuVote-TSX_Pollworkers_Guide_Rev_12.0. Note to reviewer: a ballot encoded with 'Audio' can be voted on an AccuVote-TS unit installed with VIBS hardware or UAID hardware. The Hidden option is only used when encoding and Audio ballot for use on an AccuVote-TS unit installed with VIBS hardware when the voter does not want the visual ballot to	Rejected: CAC 05/25/2009 Rejected: CAC 06/1/2009 Rejected: CAC 06/2/2009 Accepted: DEV 07/02/2009: Retried the cancellation procedures and was able to get both the TSX and TS R6 ballots to cancel. Using the force gauge at close to 5 Newtons, and pressing the button for more than 10 seconds cancelled the ballot Normal touch-screen functions do not even register on the force gauge but the force required is within the vol 1. Section 2.2.7.2.f.3 requirement.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						Audio mode) constantly. Basically, a non-VIBS user gets a ballot cancel timeout but a VIBS user does not. What happens with "fleeing voter" for a VIBS user? Reboot BallotStation is the only way I know to get the ballot to "cancel". Rejected: 06-02-2009 CAC: The UAID connected to BallotStation WITH display on also does not timeout. Rejected: 6/11/2009 KM: The updated documentation does not address the issue of the voting session not timing out after 180 seconds. SS 6/17/2009: Based on review of the the BallotStation User's Guid 4.7.5 or later Revision 2.0 dated May 25, 2009 and AccuVote-TSX Pollworker's Guide Revision 12.0 dated May 25, 2009, the ballot cancel is addressed; however, the documentatino does not address the issue of the voting session not timing out. Rejected: DEV 06/22/2009: Verified in Section 8.4.1 of the AccuVote-TS R6 Pollworker's Guide Revision 7.0 states, " The unit does not time out after 150 seconds of inactivity is detected when voting a Hidden or non-Hidden Audio ballot. If a voter voting a Hidden or non-Hidden Audio ballot leaves or flees while voting, the ballot must be manually cancelled by a pollworker. However, the 'manual' cancellation of the audio ballot did not work either. The page button was held down for 10 seconds and the cancellation screen did not appear We then held the page button down for 30 seconds and the cancellation screen still did not appear.		be displayed.	
84	5/19/09	D. Valdez	Functional Defect	Closed	AutoMARK VAT	The magnify and high contrast settings can only be selected by touching the screen. These settings cannot be accessed using a accessibility device and/or the	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-05-27] PH: I have not been able to recreate this problem. I loaded the 1.3.3418 build and was able to access zoom and high contrast by using a 2-switch	Accepted: CAC 5/28/2009: Retested and verified. Attributed to tester error.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						forward/back/next buttons on the VAT.		paddle. It's true that this functionality cannot be accessed using the keypad, but that is working as designed.	
85	5/19/09	C.Cvetezar	Functional Defect	Closed	GEMS 1.21.1Reference Guide; 6.1.10. @district	During FCA execution of GEN03, the @district macro function yielded @error results instead of the specified district. Simple election sent by Premier worked fine. The GEN03 database is available for investigation. Rejected: 05-22-2009 CAC: Investigating further, if the district Label and Tag contain different text upon creation then this function works properly; however, if the district Label and Tag contain the same text upon creation then the function gives @error... . If different text was used AFTER this creation then the error still exists. Nothing in the TDP dictates setting Label and Tag text. Rejected: 06-15-2009 CAC: using macro-ibeta.dbf for testing instead of GEN03 due to its simplicity of giving the error.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-06-15] TT: Noted error that occurs when an @district macro is used on a ballot generated for a district that is not within the parent district specified by the macro. See section 6.1.10, @district in the GEMS Reference Guide 1.21.3 or later Rev 3.0.	Rejected: CAC 05/22/2009 Rejected: CAC 06/15/2009 Accepted: CAC 07/01/2009: Validated during GEMS-R85 regression testing; @district and @precinct macros function as stated in the GEMS Reference Guide 1.21.3 or later sections 6.1.10 - 6.1.11, dated June 26, 2009.
86	5/22/09	J.Patterson	Functional Defect	Closed	GEMS 1.21.3, Volume Test VOL02b, Step20 ->SOVC	The supplied machine failed to have enough memory to run jurisdiction wide SOVC. All districts had to be printed separately, and no overall view was available.	V1: 2.5.2 All systems shall provide a means to consolidate vote data from all polling places, v2: 6.2.3 For all systems, the total number of ballots to be processed by each precinct counting device during these tests shall reflect the maximum number of active voting positions and the maximum number of ballot styles that the TDP claims the system can support.	[2009-06-10] RP: BUG#10146; fixed in GEMS 1.21.3.1	Accepted: DEV/CAC 07/01/2009: Validated during VOL2b regression testing that jurisdiction wide SOVC was able to print.
87	5/22/09	D. Valdez	Functional Defect	Closed	Premier Central Scan PhotoScribe 900 iM2, OCS version 2.2.2, GEN04a, Step 22	The DRS is only reading one ballot at a time, after which the following message is received, "Crash in main transport." Attempted to read five more ballots, one at a time, and the same message was received with an additional message stating, "Sheet Lost in Hopper 1." PCS was shutdown and restarted and the DRS displayed read, "Purge failed in	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-06-03] TT: Addressing the 'Additional information' section of the issue: How to calibrate the doubles detector is documented in section 3.4.1 of the PhotoScribe PS900 iM2/PS960 Hardware Guide Rev 7.0. (The value is not 'entered'; the user is to use the Calibration Wizard and feed an election ballot through the	Accepted: CAC 5/28/2009: Observed resolution from Irene (IS). DRS scanner functions properly.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						SheetinAcceptDet." Attempted to read additional ballots and received a message stating, "Separator Motor Faulty." None of the ballots scanned were read. Additional information: When other DRS units were maintenanced, iBeta was told the doubles detector should be set between 230 and 240. The doubles detector levels are 646-693, but no instructions were provided on how to adjust them.		scanner.) I suspect the person who wrote the discrepancy was actually referring to the Sheet Separator Gap Size, which is a space that can be adjusted using the Pad Adjustment software. The gap setting is unique, and must be defined for each scanner. Instructions for setting the gap size are provided in section 3.4.3 in the same document. [2009-06-10] TI: With respect to the incorrect double detect values, Irene reported that iBeta tester was looking at the wrong number. [2009-06-11] IS: Checked the rules for the Scanner in PCS and it was missing some of the rules and some were in red.I went to Calibration and the Image Head calibration box was missing. . I deleted the scanner from PCS, then re-started the DRS, verified the option view keys were enabled, then did the automatic calibration on image heads. The "Crash in main transport" means that the ballot did not know which bin to go to, so it stops there. (indication of rules profile errors). If ballot pulled out of hopper area instead of 'purged' you will get the "Sheet lost in Hopper 1" message and the "Purge failed in heetinAcceptDet". In order to completely clear out the path and messages, you need to "purge" using the green button several times.	
88	5/26/09	K. Wilson	Functional Defect	Closed	Key Card Tool 4.7.2 User's Guide Revision 1.0 VCProgrammer 4.7.2 User's Guide Revision 1.0	Section 1.0 and 8.1 refer to the Key Card Tool's PC but do not specify the system configuration. When Key Card Tool is run on a PC that does not have a serial port, with a USB-to-Serial device connected, the converter device chose COM3 as the port number. Key Card Tool could not run because it only shows COM1 and COM2 in the dropdown	V1: 2.2.1.f If access to a system function is to be restricted or controlled, the system shall incorporate a means of implementing this capability.	[2009-06-05] TT: COM port options are fixed (hard coded) in VCP and KCT. KCT supports COM1 and COM2 only; VCP supports COM1 to COM4 ports only. This information will be provided in the VCProgrammer User's Guide 4.7.4 Rev 2.0 and Key Card Tool User's Guide 4.7.4 or later Rev 2.0.	Accepted: DEV 06/19/2009: Verified Key Card Tool User's Guide 4.7.5 or later states Key Card Tool supports the use of COM1 or COM2 ports only and VCProgrammer

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						and in automatic detect mode still fails to find either the COM3 port or the card reader device. Similarly, on VCProgrammer, the device chooses COM5 and only COM1 through COM4 in the dropdown.		[2009-06-10] TI: The PowerEdge severs supplied have at least one serial port on board and those are the ports that should have been used not a USB to serial port adapter. All systems supplied by Premier for use with KeyCardTool or VCProgrammer have the appropriate serial ports installed.	User's Guide 4.7.5 or later states COM1 to COM4 serial ports only.
89	5/26/09	L. Laboe	Documentation Defect	Closed	OSX source code to protect against the failure of the PCMCIA data files.	The AccuVote-OSX 1.2.1 TDP documents as out of scope and review of the OSX code confirms that the OSX application does not do any checking in the code itself of any checksum or CRC of the data on the PCMCIA card. How does the OSX protect against the failure of the PCMCIA storage device? 06-11-2009 K.Wilson/CAC - request documentation stating that the lower-level errors from SQLite are obtained by the application-level error handler.	V1: 2.1.4.e Protect against the failure of any data input or storage device.	[2009-06-10] RP: Verification of the integrity of the database files used by the OSX is a function of the COTS SQLite database library, not an application-level function. If the integrity of the database is compromised, corresponding errors are returned by the SQLite library and eventually turned into application-level _com_error exceptions. [Nel, 2009-06-18] NF: The preceding text has been provided as response to section 2.3.2.4.1, Common Standards in AccuVote-OSX Software TDP 2.03 System Functionality Description.	Accepted: GA 6/29/2009: Based on review of section 2.3.2.4.1e of AccuVote-OSX Software TDP System Functionality Description Revision 2.0 dated June 16, 2009 closes this discrepancy. The explanation provided in the discrepancy response has been added to the TDP.
90	5/25/09	K. Wilson	Functional Defect	Closed	Security Test Case execution of requirement v1: 2.2.4.1.j on the AVTS tab.	The requirement for reporting the system status is interpretted to be that the audit log contains the version of BallotStation. No version information appears in the Machine audit log. A SHA appears but this is the SHA of the ABasic Report file. This SHA did not change between version 4.7.4 and 4.7.5 so it does not necessarily correlate to the BallotStation version installed.	V1: 2.2.4.1.j. Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability	[2009-06-06] IG: Incorrect. BS version is presented under the 'Machine' portion of Audit Log (as 'Release: 4.7.5').	Accepted: CAC 06/11/2009 Verified audit printout contains B.S. version under Machine of Audit Log.
91	5/26/09	K. Wilson	Functional Defect	Closed	Security Test Case execution of requirement v1: 2.2.5.3 on the AVTS tab.	No audit log of unsuccessful attempts to authenticate with the supervisor card during firmware upgrade. Also observed during this test: The paper tape contains information about the upgrade, but contains no date and time (which in the case of a field upgrade, the system probably knows). The system audit log contains no events relating to firmware upgrade or the version number before and after installation.	V1: 2.2.5.3 para 5 ... the system shall be configured to execute only intended and necessary processes during the execution of election software. V1: 2.2.4.1.g: Record and report the data and time of normal and abnormal events;	[2009-06-10] TI: Will be fixed in AVInstaller [2009-06-22] WL: Fixed in AVInstaller 1.0.1.1, which will be included in BootLoader 1.3.11.	Accepted: CAC 06/26/2009: Retested installing all firmware and verified with trusted builds (BootLoader 1.3.11 & AVInstaller 1.0.2, AVValidator 1.0.1) that date/time and versions are printed on the paper tape of

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
									firmware installs (WinCE, AVInstaller, AVValidator and BallotStation).
92	5/28/09	C.Cvetezar	Documentation Defect	Closed	Source Code - CardElement.cpp and SOCV.cpp	Source code has references to the GEMS macros @precinct and @race but the TDP only has a reference to @district macro.	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.	[2009-06-03] TT: See section 6.1.11, @precinct in the GEMS Reference Guide 1.21.3 or later Rev 2.0.	Accepted: KM 6/11/2009: GEMS_Reference_Guide_1.21.3_or_later_Rev_2.0 has references for @race and @precinct.
93	6/1/09	G.Audette	Documentation Defect	Closed	BallotStation Administrator's Guide 4.7.5 or later, Revision 1.0	When attempting to updated the TS-R6 with the 4.7.5 Trusted Build, three machines would not install the update. It was later learned that the machines running on battery power at less than 50% would not upgrade but once plugged into the wall outlet, the updated application could be loaded. 6/11/2009 KM: In Process. The BallotStation_System_Administrators_Guide_4.7.5_or_later_Rev_2.0 makes no reference to battery charge levels required to perform the upgrade.	v2: 2.4.1.e: ..and any additional facilities or resources required to install and operate the system.	[2009-06-19] TT: Revised document. Added note that AccuVote-TS units cannot be upgraded while running on battery power. See the BallotStation System Administrator's Guide Rev 3.0	Accepted: DEV 06/22/2009: Verified BallotStation System Administrator’s Guide 4.7.5 or later Revision 3.0 June 19, 2009 states, "Note: Ensure the unit is plugged in to a power source. The AccuVote-TS unit's firmware cannot be upgraded while the unit is running on battery power."
94	5/28/09	K. Wilson	Functional Defect	Closed	Security Test AVOS	AVOS-PC supervisor logon is not recorded in the audit log. Failed supervisor logon also not recorded. Once logged on, supervisor re-open polls is logged (as "count restarted"). Rejected: 6/30/09 GA: The VSTL interprets successful and unsuccessful login attempts as security events. We understand Premier's position that this is a "non-event" as it does not affect data and recommend referral to the EAC for determination of whether logging in as an Supervisor on the AVOS-PC is or is not an "event".	V1:2.1.4.g Record and report the date and time of normal and abnormal events;	[2009-06-29] TRI: All events that affect data are logged. Entering supervisor mode is not logged since it in of itself does not affect data. However events within supervisor mode that affect data are logged.	Rejected: GA 6/30/2009 Accepted: CAC 07/06/2009 - Validated during AVOS-PC-R94 regression testing of AVOS-PC 1.96.12; trusted build with this code change resolved the issue.
95	6/1/09	K. Wilson	Functional Defect	Closed	Security Test AVOS (CC Version 2.0.13)	Version of AVOS-CC does not appear in GEMS log or in paper tape of AVOS-CC.	V1:2.1.4.jInclude built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability.	[2009-06-10] TI: Will be fixed in AVCC.	Accepted: CAC 06/30/09: Validated during GEN02-R regression testing

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
									of AVOS-CC 2.0.14.
96	6/1/09	S. Sivixay	Functional Defect	Closed	VOL01 Test Case TS-R6 BS 4.7.5 and GEMS 1.21.1 Election Administrator's Guide Revision 1.0, Appendix A	While running the Logic and Accuracy test on two TS-R6 units a message was received stating "The following error has been detected: Out of Storage space". The volume test case contained 1000 precincts and the TS-R6 unit is showing Main Storage: 106 MB (87% free), Back up Storage: 3 MB (40% free) in the system information field.	V1: 2.3.4.1.d Verify that all hardware and software function correctly. v2: 4.3.5: Volume tests: These tests investigate the system's response to processing more than the expected number of ballots/voters per precinct, to processing more than the expected number of precincts, or to any other similar conditions that tend to overload the system's capacity to process, store, and report data.	[2009-06-06] TI: System responded correctly and informed the user it was out of storage space.	Accepted: GA 6/18/2009: System limit was exceeded and informed the user with an error message - closed.
97	6/2/09	C.Cvetezar	Documentation Defect	Closed	GEMS User's Guide 1.21.3 or later Revision 1.0 section 3.4.1	Document does not address the "Administrator" checkbox when adding a new user. The TDP also does not address the privilege difference for the admin vs. the non-admin user.	V1: 2.2.1.: System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security, all systems shall: … b) Provide system functions that are executable only in the intended manner and order, and only under the intended conditions	[2009-06-03] TT: See section 3.4, Users, in the GEMS User's Guide 1.21.3 or later Rev 2.0. Revised to describe functionality of Administrator checkbox.	Accepted: KM 6/11/2009: The GEMS_Users_Guide_1.21.3_or_later_Rev_3.0 explains the admin checkbox and the special features the admin user has.
98	6/2/09	C.Cvetezar	Functional Defect	Closed	AIMS (1.3.552)->Tools->Set Password… AIMS (1.3.552)->Tools->Audit Log AIMS (1.3.552)->Export->Election to Flash Card	Failed attempt to change election password was not logged in the audit log. Note: Successful attempt to change election password was logged. Attempts were: 1) Export to empty CF card. 2) Export to non-empty CF card. 3) Export to/from storage folder. Election data validations were logged; however, there was no clear log entry of the Export or Export errors themselves.	V1:2.2.4.1g: Record and report the date and time of normal and abnormal events;	[2009-06-19] SL: Will be fixed in AIMS or VAT.	Accepted: CAC 06/24/2009: Same as #101 below
99	6/2/09	C.Cvetezar	Functional Defect	Closed	AutoMARK->Test Mode->System Mainenance <password> Operations Log	There is no entry in the Operations Log that indicates an invalid password was entered when an attempt was made to enter System Maintenance.	V1:2.2.4.1g: Record and report the date and time of normal and abnormal events;	[2009-06-06] IG: Incorrect. Confirmed that invalid password login is logged in the Operations Log.	Accepted: CAC/DEV 06/11/2009: Verified that the incorrect password login attempt was entered in the Operations Log.
100	6/3/09	K. Mathis	Documentation Defect	Closed	AccuVote-OS AccuFeed Hardware Guide Revision 6.0	After processing 2800 ballots, the AVOS failed with error "IRS19:D68F:0014, Call For Service" which indicates that there was a static shock (signal conditioner was placed in-line with the power supply to verify that the error was not	IEC 61000-4-2 (1995-01) and vol.1 sect. VSS 3.2.2.8./VVSG 4.1.2.8 Verify vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand ±15 kV air discharge and ±8 kV contact discharge without	[2009-06-15] TT: Added requirement to place the AccuVote-OS unit installed with the AccuFeed on an antistatic mat to avoid building up a static charge that could disable the unit. See section 3, Installing and AccuFeed	Accepted: SS 6/17/2009: Based on review of the updated TDP and running with a mat for the remainder of the test without

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						caused by a power surge). The static build up and error was repeated. The AccuFeed manual does not specify that the unit must be placed on a grounded surface to avoid building up a static charge that will disable the AVOS-CC and cause the loss of accounting of all ballots that have been scanned since the last time the deck was committed.	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. IEC 61000-4-11 (1994-06) and vol.1 sect. VSS 3.2.2.5./VVSG4.1.2.5 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: a. Surges of 30% dip @10 ms; b. Surges of 60% dip @100 ms & 1 sec c. Surges of >95% interrupt @5 sec; d. Surges of +15% line variations of nominal line voltage; and 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	in the AccuFeed Hardware Guide Rev 7.0.	encountering the same problem, this discrepancy is closed.
101	6/5/09	D. Valdez	Functional Defect	Closed	Security Test, VAT/AIMS	During the Security test in the AIMS portion, per the test step the attempt to delete an election or change the password and then verify that this event was logged failed. The failed attempt to change election password was not logged. A successful attempt to change election password was logged.	V1:2.2.1.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.	[2009-06-19] SL: Will be fixed in AIMS or VAT.	Accepted: CAC 06/30/2009: Validated during GEN02-R regression testing of AIMS 1.3.571 with PVR 1.3.3460.
102	6/5/09	D. Valdez	Functional Defect	Closed	Security Test, VAT/AIMS	During the Security test, an attempt to change the date through system maintenance menu with invalid password was attempted pre the test step. The expected result was that the date change was not possible and there is an entry in the log of the invalid password. The actual result was that there is no entry in the Operations Log that indicates an invalid password was entered.	V1:2.2.4.1.g Record and report the date and time of normal and abnormal events;	[2009-06-19] SL: Will be fixed in AIMS or VAT.	Accepted: CAC 06/30/2009: Validated during GEN02-R regression testing of AIMS 1.3.571 with PVR 1.3.3460.
103	6/5/09	K. Wilson	Documentation Defect	Closed	Security Test, ExpressPoll tab, test preparation	After installing ExpPollUpdate.exe and ExpPollCardWriter.exe onto both the ExpressPoll 4000 and ExpressPoll 5000, there was no indication from the user interface that the appropriate firmware was installed. Likewise no version was displayed when the device was restarted. We are otherwise unable	v2:2.6.4 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	[2009-06-18] TT: Added instructions for confirming the build date of CardWriter 1.1.6. See section 5.7.2, in the ExpressPoll Administrators Guide for Version 2.0 and 2.1 Revision 5.0	Rejected: CAC 6/10/2009 Accepted: CAC 07/01/2009: Validated instructions documented in ExpressPoll

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						to determine if the installation was successful. Rejected: [06-10-2009 CAC] Now able to verify CardWriter software install with undocumented procedure that allows us to view the installed files in the IPCM folder.	information shall address software installation for all system components. also v1:8.1.1 Configuration management addresses a broad set of record keeping ...These activities include ... • Identifying discrete system components and V1:6.4.1.a 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;		Administrators Guide for Version 2.0 and 2.1 Revision 5.0, section 5.7.2, dated June 18, 2009 confirms build date of CardWriter 1.1.6.
104	6/5/09	K. Wilson	Documentation Defect	Closed	ExpressPoll Administrator's Guide Version 2.0. and 2.1 Revision 3.0 February 8, 2008 sec 5.7	The "ExpressPoll Update.cab" referred to in section 5.7 step 4 was not created as part of the ExpressPollCardWriter 1.1 Build Process Version 9.0 February 23, 2009.	v2:2.6.4 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.	EAC Response: The EAC issued a decision letter on 6/19/09. That direction is to use the Premier instructions to create the XML files to run the ExpressPoll Cardwriter testing without the ExpressPoll Update.cab.	Accepted: GA 6/26/2009: Based on the EAC direction, iBeta will test the ExpressPoll CardWriter without the ExpressPoll Update.cab as part of the regression test suite. This discrepancy is closed.
105	6/8/09	D. Valdez	Documentation Defect	Closed	ASSURE Security Manager User's Guide 1.2.2 or later, Revision 2.0, April 20, 2009	The Modify Person dialog box – Image tab, section 3.3.5, does not specify image type(s) (gif, tif, spg), any size limitations, or croppings.	V2: 2.8.4. a. Provides a detailed description of all input, output, control, and display features accessible to the operator or voter.	[2009-06-15] TT: Added list of supported image file formats to ASM User's Guide 1.2.3 or later Rev 1.0. Document to be delivered.	Accepted: SS 6/17/2009: Based on review of the updated TDP, this discrepancy is closed.
106	6/3/09	C.Cvetezar	Documentation Defect	Closed	GEMS 1.20.2 Election Administrator's Guide REv 3.0, GEMS 1.21.1 User's Guide Rev. 3	Documentation nor the software instructs users to change passwords after initial login. Rejected: [06-09-2009 CAC] When a GEMS administrator creates a new user, the user is not instructed by documentation nor the software to change their password after initial login.	v1:6.2.2 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	[2009-06-15] TT: Added requirement to change user passwords at first login. See section 3.4, Users, in the GEMS User's Guide 1.21.3 or later Rev 4.0. Document to be delivered.	Rejected: CAC 6/0/2009. Accepted: SS 6/17/2009: Based on review of the updated TDP a note has been added informing All users must change their passwords after initial login. User's Guide 1.21.3 or later Rev 4.0, this discrepancy is

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
									closed.
107	6/8/09	J.Patterson	Functional Defect	Closed	PCS - Deck Status Change - Tally	When scanning ballots; the operator can close and commit decks, but only the first of ten decks is tallying on the PS-960 and only the first nine of ten desks are tallying on the PS-900.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-06-10] SL: fixed in PCS 2.2.2.1	Accepted: DEV 06/30/2009: Retested in Volume 1 Regression by running 10 decks with 10 ballots in each deck on three different units, on PCS version 2.2.3 and all 30 decks, closed, committed, and tallied. PCS is working as designed/documented.
108	6/8/09	J.Patterson	Functional Defect	Closed	PCS - Deck Status Change - Rollback Totals	On the PS-960; the status of a deck does not change after the Rollback Totals option has been selected, thus not allowing the deck to be deleted.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-06-10] SL: fixed in PCS 2.2.2.1	Accepted: DEV 06/30/2009: Added an 11th deck, to the test run in discrepancy #107. This deck was closed, committed, and tallied. Once tallied, the totals were "rolled back" and the status change to closed. Once closed the deck was deleted. PCS is working as designed/documented.
109	6/8/09	J.Patterson	Functional Defect	Closed	PCS -> GEMS - Uploading Runs	PCS 2.2.2 or later Users Guide, section 8.2 states: 'Results of different runs uploaded for the same central count vote center will be merged in GEMS. When attempting to get 2 runs from a single vote center to upload and merge, the second run is overwriting the first. This is being seen on 3 separate DRSs, 2 PS-900 and 1 PS-960, and is reproducible on all machines. Reproduction Process: 1. Load GEMS with a backup of the election 2. Start AVServer 2. Start Central Scan software	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-06-09] IG: Invalid. Confirmed by performing steps specified in that discrepancy. It works fine as expected. Uploaded results from a different Run overwrite a previously uploaded results. [2009-06-10] SL: It works as expected. Results for all runs are merged in GEMS unless the runs have results for the same counterbatch. In this case, counterbatch results will be overridden. This exception will be added to the user documentation. [2009-06-15] TT: Revised PCS	Accepted: DEV 06/19/2009: Verified the addition of the cited notation section 2.2 of the Premier Central Scan System Administrator's Guide 2.2.3 or later and section 3.6 of the Premier Central Scan User's Guide 2.2.3 or later.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						4. Load the workspace 3. Create and select a new run - Run 4 4. Scan a deck of 100 ballots 5. Close and commit the deck 6. Create and select a new run - Run5 7. Scan the same deck of 100 ballots 8. Close and commit the deck 9. Close both Runs 10. Upload Run 4 11. Check the totals - will increase by 100 12. Upload Run 5 13. Check the totals - number stays the same		User's Guide 2.2.3 and later Rev 1.0, and PCS System Admin Guide 2.2.3 and later Rev 1.0 to indicate results for an uploaded counter batch will be overwritten if new results for the counter batch are uploaded.	
110	6/5/09	D. Valdez	Documentation Defect	Closed	ASSURE Security Manager (ASM), version 1.2.2	The ASM User's Guide states, "ASM and PCS support the DigitalPersona U.are.U® 4000B fingerprint reader;" however, we were only provided with the DigitalPersona U.are.U® 4500 fingerprint reader. Windows recognizes the 4500; but ASM does not. Under the modify person window, fingerprint tab the finger to scan selection is made, enroll button selected, and it states to attach a fingerprint scanner.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-09-11] IG: The corresponding drivers for fingerprint device supposed to be installed on ASM machine. ASM User's Guide is updated in this regard. [2009-06-15] TT: Noted support for DigitalPersona 4500 fingerprint reader in ASSURE Security Manager Users Guide 1.2.3 or later Rev 1.0 and PCS User's Guide 2.2.3 and later Rev 1.0, and to PCS System Admin Guide 2.2.3 and later Rev 1.0. Also noted required driver, and that this driver can be obtained from Premier.	Accepted: SS 6/17/2009: Based on review of the updated TDP document now mentioned the drivers needed and how to obtain them if needed, this discrepancy is closed.
111	6/8/09	C.Cvetezar	Functional Defect	Closed	ASM->localhost->Applications->Central Scan->Privileges	After ASM connect to localhost, logged into localhost as Adjudicator (adjudicator!1). This user had the ability to select localhost->Applications->Central Scan->Privileges and freely add itself to any of the privileges listed (such as Delete Decks->Access Control->Add). Note: Accepted that this user was unable to access People properties or add Roles or Role privileges. Rejected: 06-11-2009 DEV: The Adjudicator user had the following privileges: Application login; Change (assume) workspace ownership; Commit	v1:2.2.1.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		Rejected: DEV 06/11/2009 Accepted: CAC/DEV 6/12/2009: Adjudicator had edit rights on the Central Scan application itself; once that privilege was removed, Adjudicator could not access the People properties.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						decks; Adjudicate marks; Adjudicate ballots; and Upload results. The Adjudicator user also had "Edit" capabilities under access control.			
112	6/8/09	C.Cvetezar	Documentation Defect	Closed	ASM TDP	TDP does not address Failure Acceptance Rate (FAR) nor Failure Rejection Rate (FRR) for the fingerprint system.	v1:6.2.1. General Access Control Policy, 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: h. Any additional relevant characteristics.	[2009-06-11] NF: Section 2.6.1.1, General Access Control Policy (h) in ASM TDP 2.06 System Security Specification has been amended to include a reference to Appendix B: Fingerprint Reader FRR and FAR ratios in the ASM User's Guide.	Accepted: GA 6/30/2009: Based on review of the updated TDP, this discrepancy is resolved.
113	6/9/09	K. Wilson	Documentation Defect	Closed	Pending document review to find this vulnerability documented. Found in Security Review Test tab AVOS 1:2.2.1.d	The Premier Wire seals manufactured by E.J. Brooks have a problem in that if they are not applied snuggly then the wire can be cut and reinserted without leaving any obvious evidence that the wire was cut (disassembling the device would show the cut wire and one might also see the multiple frayed wire ends inside the device)	v1:2.2.1.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.	[2009-06-17] TT: Added instructions to ensure that are wire seals are properly applied and tightly secured. See section 4, Voting equipment, in Premier's Client Security Policy document Rev 6.0.	Accepted: DEV 06/22/2009: Verified in Premier's Client Security Policy, Section 9.1 the addition of the statement, " Ensure that all wire seals are properly applied and tightly secured." We also attached a seal as tight as possible and verified the seal could not be re-attached thus leaving evidence the seal/unit had been tampered with.
114	6/9/09	D. Valdez	Functional Defect	Closed	Premier Central Scan (PCS 2.2.2), Scanning Decks (Security test case, GEN04b database)	The test case was executed as written and is as follows: Need 4 decks, all different by at least one ballot. Scan the first Deck (A)>Close Central Count Server>Restart Central Count Server>Scan 2 more decks (B,C)>Scan a 4th deck (D)>unplug the DRS computer in the middle of this deck. Repower the DRS and delete the deck>Rescan the deck (D,2). Verify the tally. Verify the audit log shows that Deck D was deleted. When the DRS unit was powered an	V1:2.1.3.b Resumption of normal operation following the corrections of a failure in a memory component, or in a data processing component, including the central processing unit;	[2009-06-17] TT: See section 3.1, Configuring connections, in the PhotoScribe_PS900_iM2_PS960_Hardware_Guide_Rev_8.0. Instructed users to use an UPS device. See section 3.2, Powering the unit on and off, in the same document. Instructed users not to power off the scanner while uploading/downloading to GEMS, or while processing ballots for a workspace. Added the same information to Section 4, General PCS Operating Procedures, to the PCS User's Guide 2.2.3 or later Rev 2.0.	Accepted: DEV 06/19/2009: Verified the DRS PhotoScribe PS900 iM2/PS960 Revision 8.0 June 16, 2009 Hardware Guide and Premier Central Scan User's Guide 2.2.3 or later state to plug the scanner into an Uninterruptable Power Supply (UPS) device and not turn the unit

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						error message was received (screenshot available). We clicked OK on the error, the Workspace loaded and we were able to activate the Workspace; but none of the three scanned decks appeared. A new run was created and the steps were followed again, but this time we committed each scanned deck (three total). When the DRS unit was powered on, the same error was received, we clicked OK on the error, the workspace loaded, the error was received again, but we were unable to activate the Workspace. All scanned decks were lost.			on/off while downloading or uploading to GEMS or a loss of data will occur.
115	6/11/09	C.Cvetezar	Functional Defect	Closed	DRS PhotoScribe PS900/960	There is no battery backup (up to 5 minutes) on the DRS PhotoScribe PS900 & PS960 scanners. DEV 06/19/2009: The DRS PhotoScribe PS900 iM2/PS960 Revision 8.0 June 16, 2009 Hardware Guide and Premier Central Scan User's Guide 2.2.3 or later state to plug the scanner into an Uninterruptable Power Supply (UPS) device; however, does not mention the UPS must power the scanner for five minutes.	v1: 3.2.2.4c 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. v1: 3.2.2.5 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: a. Surges of 30% dip @10 ms; b. Surges of 60% dip @100 ms & 1 sec c. Surges of >95% interrupt @5 sec; d. Surges of +15% line variations of nominal line voltage; and 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. RFI 2008-06 Central Count Battery Back-up 2009-06-15 C.Cvetezar: As per EAC Decision on Request for Interpretation 2008-06 (Battery Back Up for Central Count): The graceful shutdown shall meet the following requirements: 1. All ballots shall reside in either the input or output hopper with no ballots	[2009-06-29] TT: See section 3.1, Configuring connections, in the PhotoScribe_PS900_iM2_PS960_Hardware_Guide_Rev_9.0. Instructed users to use an UPS device capable of providing a minimum of 5 minutes of uninterrupted power in the event of power failure. Added the same information to Section 4, General PCS Operating Procedures, to the PCS User's Guide 2.2.3 or later Rev 3.0.	Accepted: GA 6/30/2009: Section 3.0 of Revision 9.0 of the PhotoScribe Hardware Guide dated 25 June 2009 and Section 4.0 of Revision 3.0 of the PCS User's Guide dated 25 June 2009 contains the 5 minute requirement per RFI 2008-06.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
							in process at the end of the shutdown process. 2. All ballots in the output hopper shall be fully read and saved. 3. A report, including the final state of all ballots, timestamps and of the final state of the unit, shall be printed or saved in a file. The report shall be part of the permanent election record and shall be available when power is restored to the system. 4. The system shall be capable of resuming operation from the point it stopped once power is restored.		
116	6/11/09	C.Cvetezar	Functional Defect	Closed	PCS->workspace->download	Powering off the PC running PCS software during a workspace download corrupted the workspace and did not recover upon power up. The workspace is unusable.	V1:2.2.3 a. Restoration of the device to the operating condition existing immediately prior to the error or failure, without loss or corruption of voting data previously stored in the device; b. Resumption of normal operation following the corrections of a failure in a memory component, or in a data processing component, including the central processing unit;	[2009-06-17] TT: See section 3.1, Configuring connections, in the PhotoScribe_PS900_iM2_PS960_Hardware_Guide_Rev_8.0. Instructed users to use an UPS device. See section 3.2, Powering the unit on and off, in the same document. Instructed users not to power off the scanner while uploading/downloading to GEMS, or while processing ballots for a workspace. Added the same information to Section 4, General PCS Operating Procedures, to the PCS User's Guide 2.2.3 or later Rev 2.0.	Accepted: DEV 06/19/2009: Verified the DRS PhotoScribe PS900 iM2/PS960 Revision 8.0 June 16, 2009 Hardware Guide and Premier Central Scan User's Guide 2.2.3 or later state to plug the scanner into an Uninterruptable Power Supply (UPS) device and not turn the unit on/off while downloading or uploading to GEMS or a loss of data will occur.
117	6/11/09	C.Cvetezar	Documentation Defect or Functional Defect	Closed	Premier Central Scan User's Guide 2.2.2 or later Revision 3.0, section 3.8. Defining Scanners, 3. If a scanner is connected to a workstation using a COM port, enter the name of the port in the Startup	Adding a network scanner (using IP address) is not addressed in the Premier Central Scan TDP. Unable to add a DRS Photoscribe scanner to PCS that is running on a PC server (XP) connected to a network hub.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.		Accepted: DEV 6/18/2009: Discrepancy has been closed as an invalid test/test case error.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
					parameters field. For example, enter COM1:				
118	6/11/09	C.Cvetezar	Documentation Defect	Closed	FEC 2002 VCProgrammer Technical Data Package Appendix F: System and Data Integrity, 5.1 Activation Code	VCProgrammer does not require an activation code during installation or initial software launch.	v1: 4.1.1 the vendors shall submit to the ITA, in the TDP, a record of all user selections made during software installation. v2:2.6.4 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.	[2009-06-15] NF: Section 5.1, Activation code has been removed from VCProgrammer TDP Appendix F: System and Data Integrity.	Accepted: GA 6/29/2009: Based on review of VCProgrammer Appendix F: System and Data Integrity Revision 2 dated June 16, 2009, this discrepancy is closed.
119	6/12/09	C.Cvetezar	Documentation Defect or Functional Defect	Closed	ASSURE Security Manager User's Guide 1.2.2 or later, .	Section 3.3.5: Adding images to users, The image that is associated with a PCS user (and the user's application privileges) will be displayed in a tool-tip when the mouse is rolled over the user icon in the PCS application interface 1) The Tool-Tip image would not display in PCS when mouse-over the user icon. 2) The document does not address image properties such as size and cropping as the image that was used got cropped automatically.	V1: 2.3.4.1.d Verify that all hardware and software function correctly. V2: 2.8.5.b The vendor shall provide documentation of system operating procedures that meet the following requirements: b. Provides procedures that clearly enable the operator to access the control flow of system functions (as evidenced by system...	[2009-06-17] IG: 1. Tool-Tip image appears properly fine in PCS when mouse pointer is located over the user icon. [2009-06-17] TT: Added list of supported image file formats to ASM User's Guide 1.2.3 or later Rev 1.0. Document delivered.	Accepted: CAC 06/30/2009: Validated during GEN02-R regression testing of PCS 2.2.3 with ASM 1.2.3.
120	6/12/09	C.Cvetezar	Documentation Defect	Closed	Premier Central Scan - initial launch	Upon initial launch of PCS, Windows prompted for a validation of a user run the application. ASSURE_USER with password had to be selected before application would run. This is not addressed in any documentation in the TDP. Screenshot: PCS login.jpg	V2: 2.8.5.b The vendor shall provide documentation of system operating procedures that meet the following requirements: a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation;	[2009-06-18] TT: Instructions on how to change the password for the ASSURE_User are included in the ASSURE_Security_Manager_Users_Guide_1.2.3_or_later_Rev_1.0; instructions on how to subsequently change it are provided in ASSURE_Security_Manager_Users_Guide_1.2.3_or_later_Rev_2.0.	Accepted: CAC 06/30/2009: Validated document ASSURE_Security_Manager_Users_Guide_1.2.3_or_later_Rev_1.0.
121	6/12/09	C.Cvetezar	Functional Defect	Closed	VCProgrammer - launch	Upon launch of VCProgrammer the following error is displayed: "Exception: Failed to query registry entry InstallPath". Upon selecting OK the application runs properly.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-06-18] IG: The problem is fixed in the next VCP release.	Accepted: CAC 06/26/2009: Retested and verified trusted build 4.7.5 has no such error display upon launch.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
122	6/12/09	C.Cvetezar	Functional Defect	Closed	VCProgrammer - Card Status	Observing the Card Status line, some status text is incompletely displayed such as a Card Status of: "Card Precinct … created - Please". It is not known what the "Please" is in reference to.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.		Accepted: CAC 06/16/2009: Expanding or maximizing the Voter Card Entry screen displays the status line in totality.
123	6/12/09	C.Cvetezar	Documentation Defect	Closed	Key Card Tool - Audit Log	During security testing, trying to verify that Key Card Tool documentation contains instructions to safeguard the Key Card Tool log file(s) in the event of a system failure (when possible), there is no audit log with KCT.	v1:2.2.1.d. Provide safeguards to protect against tampering during system repair, or interventions in system operations, in response to system failure.	[2009-06-15] TT: The Audit Log is documented in the Key Card Tool User's Guide 4.7.5 or later Rev 1.0.	Accepted: SS 6/17/2009: Based on review of the updated TDP the audit log has now been included in the document, this discrepancy is closed.
124	6/12/09	C.Cvetezar	Documentation Defect or Functional Defect	Closed	Assure Security Manager - People->Fingerprint	When using the DigitalPersona U.are.U® 4500 fingerprint reader along with the 4000B drivers, the fingerprint reader must be disconnected and reconnected for each scan as the reader does not function after the first one. The TDP does not address this functional usage of the scanner.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-06-17] IG: It is not required to re-connect fingerprint for a second attempt. The finger should be scanned two or more times to be identified by Fingerprint reader.	Accepted: DEV 06/22/2009: Retested and found the scanner is more sensitive after the 'touch pad' area was wiped down and did not have to be reconnected after each use. Finger was scanned up to 10 consecutive times and never had to be disconnected. Vendor response is correct in that finger did have to be placed numerous times for the fingerprint to be recognized.
125	6/12/09	C.Cvetezar	Documentation Defect or Functional Defect	Closed	Premier Central Scan - login (with fingerprint authentication)	When using the DigitalPersona U.are.U® 4500 fingerprint reader along with the 4000B drivers, the fingerprint reader must be disconnected and reconnected for each scan that is in error (verifying fingerprint) as the reader does not function after the first one. The PCS application must also be shutdown and restarted for the reader to function again. The TDP does not address this functional usage of the scanner.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-06-17] IG: It is not required to re-connect fingerprint for a second attempt. The finger should be scanned two or more times to be identified by Fingerprint reader.	Accepted: DEV 06/22/2009: Retested and found the scanner is more sensitive after the 'touch pad' area was wiped down and did not have to be reconnected after each use and PCS did not have to restarted. Finger was scanned up to

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
									10 consecutive times and never had to be disconnected. Vendor response is correct in that finger did have to be placed numerous times for the fingerprint to be recognized.
126	6/12/09	C.Cvetezar	Documentation Defect	Closed	Voter Card Encoder - Firmware Installation	During security testing, installing firmware for the VCE required the vendor to provide the "downldr.exe" file. This COTS file needs to be documented by the vendor indicating its authentication was provided from the COTS vendor (Spyrus).	v1: 2.2.5.3 COTS General Purpose Computer System Requirements	[2009-06-24] SL: Certification for procured software: downldr.exe was authenticated and documented.	Accepted: GA 6/26/2009: A letter from Premier attesting to the procurement of downldr.exe was received and reviewed.
127	6/12/09	S.Eaton	Documentation Defect	Closed	AccuVote OS Central Count User's Guide 2.0.13 or later Revision 1.0 or 4.0 (on the revision history)	The revision number on the front page of the document and in the revision history do not match.	v1: 8.3.2 Versioning Conventions	[2009-06-15] TT: Revised revision number in document History table to match revision number on cover. See the AccuVote-OS Central Count User's Guide 2.0.13 or later Rev 1.1.	Accepted: SS 6/17/2009: Based on review of the updated TDP revision number is now matching with cover page, this discrepancy is closed.
128	6/12/09	J.Patterson	Functional Defect	Closed	GEMS -> SOVC - Print limitations	GEMS Reference Guide 10.12 states: "By default, the All radio button is selected, indicating that the entire report will be printed." When the All radio button is selected, and the report is more than 10,000 pages, GEMS will only send 9,999 pages to the printer. Workaround: Selecting a Print Range that is equal to the pages in the report sends the entire report to the printer. i.e.: The VOL01 SOVC is 24,300 pages. Selecting All sends pages 1-9,999 to the printer. Selecting a Page Range of 1-24,300 sends all pages to the printer.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-06-18] WL: Fixed in GEMS 1.21.3.3	Accepted: DEV 06/30/2009: Generated the Statement of Votes Cast in Volume 1 Regression test case, using GEMS version 1.21.4 and all 24,300 pages of the report were immediately available for preview with the default radio button selected. We no longer had to use a print range.
129	6/12/09	J.Patterson	Functional Defect	Closed	GEMS -> View Ballots -> Export limitations	While attempting to export ballots to a PDF the system returns an error stating that There are no limits to ballot	VII: 6.2.1 ITAs shall design and perform procedures that test the voting system capabilities for the system as a whole. These procedures follow the	[2009-06-09] WL: Fixed in GEMS 1.21.3.3	Accepted: DEV 06/30/2009: Tested in Volume 1b Regression test case and the ballot

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						exportation discussed in either the User's Guide or the Reference Guide.	testing of the systems hardware and software, and address voting system requirements defined in Volume I, Sections 2, 5, 6 and 8. These procedures shall also address the requirements for testing system functionality provided in Volume II, Section 3.		image report took approximately 3.5 hours to generate and generated with 19 different files. Each file has 8191 (the limitation number reached in the original discrepancy) ballot images. After the 8191st ballot images, the new files begins with the 8192nd image and all the ballot images are now viewable.
130	6/12/09	J.Patterson	Functional Defect	Closed	GEMS -> SOVC - Preview limitations	When attempting to preview a large report, the preview generated will contain a fraction of the pages that are contained in the full report. i.e.: The SOVC has a total of 24,300 pages. When the preview function is used, a message is displayed stating that the report will be 24,300 pages, but the preview generated contains 243 pages. There are no limits or discussed in either the User's Guide or the Reference Guide. Rejected (2009-06-17 JP) I checked on this and the preview is only generating 243 pages. No matter how I try to navigate it, there are only those pages showing.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-06-16] IG: In order to preview the entire SOVC report, you need to use horizontal and vertical arrow buttons. By using horizontal arrow buttons, you are navigating from race to race. By using vertical arrow buttons, you are previewing all precincts under the specific race. [2009-06-18] IG: It works as expected.	Rejected: JP 6/17/2009 Accepted: JP 6/29/2009 Tested on GEMS 1.21.4.0 - all pages are displayed in the preview as expected.
131	6/16/09	D. Valdez	Informational	Closed	TS R6 audio	The TS R6 audio quality is poor. The instructions/contests/candidates are difficult to hear over the static. Brand new headphones were used on two different TS R6 units and the sound quality was the same. The new headphones were used on the TSX and the sound quality is fine. (The TS-R6 is no longer in production.)	V1: 2.3.4.1.d Verify that all hardware and software function correctly. V1:2.7.2 d. Meet the requirements of ANSI C63.19-2001 Category 4 to avoid electromagnetic interference with assistive hearing devices; HAVA: 301.a.3 Accessibility for individuals with disabilities.--The voting system shall--a. be accessible for individuals with	[2009-06-26] TI: There is nothing in the standards that specify audio quality such as Total Harmonic Distortion or Signal to Noise Ratio. This product has been tested and passed by multiple certified labs as well as multiple state certification bodies without any issue being raised about the audio quality.	Accepted: GA 7/6/2009: iBeta agrees that there is no requirement in the VSS or HAVA for audio quality. This discrepancy has been modified to be an 'Information' defect type.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
							disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters;		
132	6/16/09	C.Cvetezar	Functional Defect	Closed	AutoMARK PVR/PAVR 1.3.3418	Party graphics do not appear on the display when programmed and exported from GEMS. Charles has the GEN03 database and AutoMARK support files.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-06-18] IG: Graphics are not specified to be included in the Rich Text export file. Graphics, if used, must be manually assigned in AIMS. See section 12.2.1, and section 7.1.3.12 in the AIMS_PREM_Sect05_Election_Officials_Guide_AQS-13-5001-209-R document.	Accepted: DEV 06/22/2009: Verified the steps provided in section 12.2 of the AIMS Election Officials Guide AQS-13-5001-209-R Information Management System Election Official's Guide to be accurate and viewed added party graphics.
133	6/19/09	K. Wilson	Functional Defect	Closed	Telephony and Cryptographic Test Case step 23	The AVServer log does not contain the machine serial number when test results were uploaded via modem for the OSX or OS-PC devices. The IP address (OSX) is insufficient to meet this requirement because the IP address might be reused as different devices phone in to the RRAS.	V1:4.4.2.g. For systems that use a public network, provide a report of test ballots that includes: 1) Number of ballots sent; 2) When each ballot was sent; 3) Machine from which each ballot was sent; and 4) Specific votes or selections contained in the ballot.	[2009-06-26] TI: The audit records include the Machine Id that the results came from. The standards do not stipulate the machine serial number.	Accepted: KGW 7/2/2009: Verified that the Machine ID which corresponds to a memory card id appears in the report.
134	6/19/09	K. Wilson	Functional Defect	Closed	Telephony and Cryptographic Test Case step 28	AVOS-PC does not encrypt, or digitally sign votes/vote counts that are transmitted by modem.	V1:6.6.1.b All systems that transmit data over public telecommunications networks shall ... b. Employ digital signature for all communications between the vote server and other devices that communicate with the server over the network; and	[2009-06-22] TI: Section 6.6.1 is a subsection of 6.6.which states: "DRE systems that transmit data over public telecommunications networks face security risks that are not present in other DRE systems. This section describes standards applicable to DRE	Accepted: GA 6/26/2009: This requirement is also for official data. Based on review of the VSS 2002 and the vendor response, this discrepancy is closed.
135	6/19/09	K. Wilson	Functional Defect	Closed	Telephony and Cryptographic Test Case step 30	Although GEMS must be in Start mode to upload vote counts (requiring the authentication of a Central Count worker) from the OS-PC and OSX, these two devices require only a Vote Ender Card to transmit votes by modem.	V1:6.6.1.c All systems that transmit data over public telecommunications networks shall ... Require that at least two authorized election officials activate any critical operation regarding the processing of ballots transmitted over a public communications network takes place, i.e. the passwords or cryptographic keys of at least two employees are required to perform processing of	[2009-06-22] TI: Section 6.6.1 is a subsection of 6.6.which states: "DRE systems that transmit data over public telecommunications networks face security risks that are not present in other DRE systems. This section describes standards applicable to DRE systems that use public telecommunications networks." The AVOS-PC is NOT a DRE	Accepted: GA 6/26/2009: This requirement is also for official data. Based on review of the VSS 2002 and the vendor response, this discrepancy is closed.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
							votes	system.	
136	6/19/09	K. Wilson	Documentation Defect	Closed	Telephony and Cryptographic Test Case step 28a	The "random number" used by AVOS-PC to generate the challenge authentication material is not random. It therefore provides no access control to data in transit over public communications networks. 6/26/09 KGW: Modified to documentation discrepancy as the use of the 'random number' prevents a replay attack but not a man-in-the-middle attack. 7/2/2009 KGW: Section 7.2 of the System and Data Integrity Rev 2, Jun 30, 2009 contains statements that the transmission is secured by generation of a "public key" from a random number. (ref System Functionality Description sec 2.3.2.1.1 Rev 1 May 2009 which references the above section 7.2). No such access control is provided by a sequence of non-random numbers. (The documentation already states that telephone transmissions must only be after the close of the polls and should always be for unofficial results). In light of the closure of #137, the AVOS-PC documentation must state AVOS-PC transmission is not protected from unauthorized access or modification except by the assumption that a point-to-point dialed telephone transmission is reasonably secure.	V1:6.5.1 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.	[2009-06-22] TI: The 'random number' is not used to provide access control. Knowing the 'random number' does not provide access to any system hardware, software, or data functions.	Rejected: KGW 6/26/2009 Rejected: KGW 7/2/2009 Accepted: GA 7/8/2009: Validated that the AccuVote-OS Precinct Count User's Guild 1.96.12 or later Revision 2.0 dated 6 July 2009 states in Section 9.2 that the connection is reasonably secure and does not depend on the random number for security.
137	6/19/09	K. Wilson	Functional Defect	Closed	Telephony and Cryptographic Test Case step 28a	Even though a 16 bit mutual challenge is performed, the remainder of the data is unprotected. The authentication prevents a replay attack (in theory, within an entropy of 16 bits and discrepancy #136) but has no effect on a man-in-the-middle attack. 6/26/09 KGW: The man-in-the-middle attack is traced to v1: 6.5.1 because if an attack is successful, there is no access control. 6/30/09 GA: v1: 6.5.1 states that	V1:6.5.1 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. V1: 6.2: (emphasis added) Access controls provide reasonable assurance that system resources such as data files, application programs, and computer-related facilities and equipment are protected	[2009-06-29] TI: As stated above, man-in-the-middle attacks are covered in section 6.5.3 of the standards and only refer to telecommunications before the polls close. Furthermore, the telecommunications features on the AccuVote-OS are dial-out only communications and therefore do not provide any additional access to the system hardware, software, or data on the system. Therefore the access controls for the system are the same with or without telecommunications.	Rejected: KGW 6/26/2009 Rejected: GA 6/30/2009 Accepted: GA 6/30/2009: Agree, based on review of the architecture and TDP, that reasonable assurance is provided and the system meets the

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						voting systems that use telecommunications are subject to the same security requirements governing access and in v1: 6.2, the unauthorized operations include abstraction of raw or processed voting data in any form other than a standard output report by an authorized operator. A man-in-the-middle attack would allow for abstraction of raw or unprocessed voting data from the transmission by the AVOS-PC.	from unauthorized operation, modification, disclosure, loss, or impairment. Unauthorized operations include modification of compiled or interpreted code, run-time alteration of flow control logic or of data, and abstraction of raw or processed voting data in any form other than a standard output report by an authorized operator.	[2009-06-30] TI: As stated above, man-in-the-middle attacks are covered in section 6.5.3 of the standards and only refer to telecommunications before the polls close. Furthermore, the telecommunications features on the AccuVote-OS are dial-out only communications and therefore do not provide any additional access to the system hardware, software, or data on the system. Therefore the access controls for the system are the same with or without telecommunications. Also the telecommunication is point to point from the internal modem of the AccuVote-OS to the modems at the election central, and is not a packet-switched network protocol. Therefore traditional man-in-the-middle attack vectors do not apply on this point-to-point communications and so this provides for a reasonable assurance of access control is maintained.	requirement.
138	6/26/09	K. Wilson	Documentation Defect	Closed	Development Administration Build Configuration Guide Rev 16.0 (2/10/2009)	Section 3.5 of Development Administration Build Configuration Guide Rev 16.0 (2/10/2009) refers to installation of mkinstall.pem as a part of the configuration. mkinstall.pem is not a COTS file and therefore can not be installed prior to the source code installation during the build process. Its appearance in this location of the documentation is therefore incorrect and/or misleading.	V1:8.8 Within this context, a vendor is required to develop and provide a complete description of the procedures and related practices for maintaining information about: ... b. Physical location of the tools, including designation of computer directories and files; and	[2009-06-29] WL: Updated Build Configuration Guide Revision 17.0.	Accepted: GA 7/1/2009: Based on review of the updated document, this discrepancy is closed.
139	6/26/09	K. Wilson	Documentation Defect	Closed	Windows CE 3.0 Build Process Rev 6.0 (5/25/2009)	Following the step on pg 3-1 to execute wince300.bat, the error message "The system cannot find the path specified WinCE SHx SH3 accuvoteets_ide\\WinCE300 AccuvoteETS Development Environment for Lauren Laboe" appeared. This error looked fatal to both the iBeta builder and the Premier witness. We found out it is normal but had to wait to continue the build.	v1:9.6.2.4 The ITA responsible for testing voting system software, telecommunications, and integrated system operation (i.e., system wide testing) shall witness the final system build, encompassing hardware, software and communications, and the version of associated records and documentation	[2009-06-29] WL: Updated Windows CE 3.0 Build Process Revision 7.0.	Accepted: GA 6/30/2009: Review of Section 3. of the Windows CD 3.0 Build Process Revision 7.0 dated 28 June 2009 addresses this error message and closes the discrepancy.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
140	6/30/09	C.Cvetezar	Functional Defect	Closed	VCProgrammer->Create Card	During GEN02-R testing, using VCP 4.7.5, creating voter cards for District D1 (pct 10 or 11): When the voter card is inserted into a TSX running BallotStation 4.7.5 (of the same election) the following message appears: "Multiple ballots were found for the current voter - please see pollworker." Screenshot, voter card data and election database are available (GEN02-R VCP card create error).	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-06-30] TT: The VCProgrammer only supports one counter group. The database you are trying to use has more than one counter group. This restriction is documented in our user guide.	Accepted: CAC 7/01/2009: Accept. Review of Section 3. of VCProgrammer System Administrator's Guider 4.7.5 or later Rev 1.0, Section 2.1 dated 15 June 2009 addresses this error message and closes the discrepancy.
141	6/30/09	C.Cvetezar	Functional Defect	Closed	GEMS->Generate Ballots	Using the database "GEN02-R - BallotLayoutPref - error.gbf" gives a GEMS application error of: "Error at .\BallotLayoutPref.cpp Line 439 Revision Jun 23 2009". Note: Setting the ballot size other than 11 inch in Elections->Ballot Options allows ballot generation. Support files: BallotLayoutPref-error-800.jpg and GEN02-R - BallotLayoutPref - error.gbf.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-07-20] DL: Bug 10183. Fixed in GEMS 1.21.5	Accepted: CAC 07/21/2009: Closed - Validated during GEN02-R_v.1 regression testing of GEMS 1.21.5
142	6/30/09	K.Wilson/CAC	Functional Defect	Closed	Security Test	As system admin, logged in and disabled system Event Log, rebooted, system Event Log was not running; GEMS, ASM , AIMS, and VCProgrammer ran fine.	V1:2.2.5.3 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.	[[2009-07-21] SL: Fixed in GEMS 1.21.5, PCS, PCS 2.2.4, ASM 1.2.4, KCT 4.7.7 and VCP 4.7.7.	Accepted: CAC 07/21/2009: Closed - Validated during GEN02-R_v.1 regression testing of GEMS 1.21.5, ASM 1.2.5, AIMS 1.3.572, VCP 4.7.8, KCT 4.7.8, PCS 2.2.5
143	6/30/09	C.Cvetezar	Functional Defect	Closed	GEMS->View Ballots->Central Count; Export button	During GEN02-R testing, using GEMS 1.21.4 and GEN02-R_Final_09-06301455.gbf, setting the format to PDF and Entries Per File to No Limit, an application error "util.h Line 1015" appears. Setting the Entries Per File to Maximum 1 does not get this error. Support files: GEN02-R_Final_09-06301455.gbf and GEN02-R BallotImage - CC util.h error.jpg.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-07-20] WL: Bug 10090. Fixed in GEMS 1.21.5	Accepted: CAC 07/21/2009: Closed - Validated during GEN02-R_v.1 regression testing of GEMS 1.21.5
144	7/14/09	K. Wilson	Functional Defect	Closed	Key Card Tool 4.7.5.1 and BallotStation 4.7.5.1	During the source code review of the updated code, the modification to use expired certificates must be logged. CBufferedSocket is used in both KCT, and Ballot Station and is	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	[2009-07-10] TI email: The decision to ignore the date on the certificates is a policy and design decision and does not contradict any requirements of the standards	Accepted GA 7/14/2009: There is not a VSS requirement that specifically requires

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						used to transmit vote counts over public telecommunications networks.	programmed events that occur without the intervention of the voter or a polling place operator	therefore ignoring the date on a certificate is not an error. This policy is documented in our user documentation.	that the dates on certificates be valid and it is understood that expiration dates are a concern to jurisdictions, as such, this defect is closed and disclosed as part of this Test Report.
145	7/17/09	C.Cvetezar	Functional Defect	Closed	PCS->Navigate->GEMS Counter Batch Totals->Start Poster->Upload Now!	During GEN02-R_v.1 regression testing, PCS failed to upload (Poster) results to GEMS: Down a Workspace (Central Count D4); Create a Run; Read in 4 ballots; Close/Tally/Commit the deck; Start Poster; Upload Now!; AVServer Audit Log event: SSL accept error: error:140890C7:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:... PCS Audit Log event: Failed to retrieve the counter batch status list from the remote host [Remote request execution failed [TallyHo.socket.1: 0x80040209 SSL handshaking failed [winsock: 0x00002746 Connection reset by peer]]] Support files: GEN02-R_ElectionCreate_09-07160825.gbf PCS - Audit Log Report bef Post.jpg AVServerLog - PCS_09-07161204.pdf (pages 2 and 3)	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-07-20] IG: Bug: 10210. Fixed in PCS 2.2.5.	Accepted: CAC 07/21/2009: Closed - Validated during GEN02-R_v.1 regression testing of GEMS 1.21.5, ASM 1.2.5, PCS 2.2.5
146	7/17/09	C.Cvetezar	Functional Defect	Closed	GEMS->View Ballots	During GEN02-R_v.1 regression testing and using the VOL01-Reg.gbf database: GEMS->View Ballots Select Central Count in the dropdown Export button Vote Center ID Range: All When entering "1" for the Entries Per File: Maximum, no file is exported.	V1: 2.3.4.1.d Verify that all hardware and software function correctly.	[2009-07-20] TT: The number of ballot records specified must be greater than or equal to the number of ballot records per vote center/MID combination. No ballot records will be printed for voter center/MID combinations with fewer ballots than the specified value. See section 12.1, View Ballots in the GEMS 1.21.3 or later User's Guide Rev 5.0 Clarified	Rejected: CAC 07/21/2009 Accepted: CAC 07/21/2009: Closed - Validated during GEN02-R_v.1 regression testing of GEMS 1.21.5 and accept vendor response.

#	Date	Tester	Type	Status	Location	Issue Description	Requirement	Premier Response	Validation
						As per GEMS User's Guide 1.21.3 or later, v4.0 dated June 15, 2009, section 12.1, it is supposed to produce PDF files of all ballot records with a maximum number of voted ballot entries per file of one. There is no file output. When entering "0" for the Entries Per File: Maximum, a warning message displays to enter an integer between 1 and 2147483647. When I try to enter 2147483647, the text box does not allow the last digit "7" (only allowed 214748364 to be entered). 2009-07-21 CAC: During regression testing, setting the Maximum Entries Per File to several different values, it is easy to get an exported PDF file that errors in Adobe Reader that the file has no pages (VC 60 - Vote Center for Test - FILE 1.pdf). An example is a database that was used, Central Count, Export, Format: PDF, Maximum Entries Per File set to 1000, Vote Center Id Range: All Id 50, MID 503 has Count of 100, 1303 to ... has Count of 15000 (or more), Id 60, MID 8 has Count of 2000, 11 to ... has Count of 1000 or less. I expected MID 11, 12, 13 of Id 60 to have entries but I get only the MID 503 of Id 50. Also setting the Maximum Entries Per File set to 1001 gives the same output files. Support Files: VOL01-Reg.gbf (backup password: premier, database user: admin, password: premiere) BallotImageExport.jpg VC 50 - Absentee - FILE 1.pdf VC 60 - Vote Center for Test - FILE 1.pdf Adobe Error.jpg Please explain in detail and examples on the function of the Maximum Entries Per File setting.		"Maximum" value. [2009-07-20] WL: The text box allows only 9 digits to be entered. [2009-07-21] WL: 2147483647 is 0x7FFFFFFF in HEX, which is the internal limit of the value it can holds. For each vote center, it goes through each batch of ballots based on the MID order. Since the number 2000 in (ID 60, MID 8) already exceeds your defined limit 1000, it stops right there. You will need to set the limit to 5000 (2000 + 2000 + 1000) or higher to start seeing the ballots in (ID 60, MID 11).	