Report Prepared for the
Texas Secretary of State
Elections Division

Voting System Certification Evaluation Report

Hart InterCivic
Hart Voting System
Version 6.2.1

Introduction

The Hart InterCivic Voting System, Version 6.2.1 (the system) was evaluated for certification as a voting system by the State of Texas on January 17-18, 2008.

Recommendation

It is recommended that this system NOT be certified until Hart InterCivic addresses the issues cited below, under Conditions of Certification. Contingent on the vendor's satisfactory meeting the conditions specified in this report, the system would be found to comply with the requirements of the State of Texas for voting systems and would then be recommended for certification in the state of Texas.

This system is one of the best voting systems that has been presented for certification in Texas. The reasons for not recommending certification may be remedied without redesigning the system but are essential to assure that the system can be operated in a secure manner.

Conditions of Certification

1. All files installed with the system must be filed with the NIST NSRL.

   Hart InterCivic's response is egregiously deficient.

   To support incoming inspection of new systems a list of all files installed is need so that the new system can be verified as having only the system as certified.

   Pre and post election checks to confirm that software has not been changed or

tampered with are recommended. To do this local jurisdictions must have HASH codes of all static files. Further, to avoid the system having a single point vulnerability the non-static files, that change with use, should be evaluated by an entity other than the vendor. Why non-static files change should be understood by state and local authorities. Election officials should make their own independent determination that files that change with use and are not included in pre and post election checks are appropriate and do not represent a security vulnerability.

2. In response to the question:

   "Beyond the files installed with the Hart software, what other files in the operating system and elsewhere do the applications in the Hart 6.2.1 system use?"

   Hart responded:

   "Like most Windows based software, System 6.2.1's HVS applications make broad use of Windows resources, including hundreds of DLLs and other executable files. Hart would be happy to provide information on the identification of each of these individual files and there respective purpose and characteristics (e.g. why does its HASH code value change from one day to the next or one install to the next), but the information was not required during the original ITA and NASED certification testing, nor during subsequent "

   In its response Hart illustrates the importance of this point. The Hart software makes "broad use of Windows resources, including hundreds of DLLs and other executable files". Each of those files represents a potential vulnerability, an opportunity to introduce malicious code into the system. For that very reason it is essential that the information be available to verify these files both in the certification process and pre and post election.

   Past deficiencies are no reason to propagate a vulnerability into the future. Being able to confirm that the software certified at the national and state level is identical to that installed and used in elections is one of the most significant improvements to total election system security that can be made. Implementing such checks requires not modification or recertification of a voting system, unlike many changes. The tools to verify HASH codes are readily available and do not require extensive training to use. It is hard to imagine why a change that is this beneficial is being resisted.

3. In its response on the HASH code issue Hart InterCivic states:

   "These criteria have been imposed on Hart HASH code submissions by arrangements agreed between Hart and NIST in the absence of other specific authoritative requirements for vendor reference files."

   This statement is inaccurate and misleading. This examiner has met personally and had multiple telephone conversations with NIST NSRL staff. NIST NSRL will HASH and post any files a vendor gives them to post.

4. Although the Hart InterCivic system is NASED certified it fails to meet some requirements for NASED certification dealing with operating system configuration. A secure configuration of the operating systems provided must be provided with instructions on how to check the configuration.

   To assure that the system is adequately secure Hart must specify an operating system configuration, with adequate safeguards to assure that the Hart applications will only run in a secure configuration of the operating system. The configuration should be consistent with industry practice as represented in the NIST security configuration checklist for its operating system, Windows 2000 Professional?[1]

   a. In its response to questions about the Hart Intercivic recommended configuration the company stated:

      "Setup and configuration of HVS application computers is accomplished only by qualified Hart technical personnel and includes all Windows updates as of the date of the install."

      This practice is not acceptable. Voting system applications use many operating system functions. Changes to the operating system should only be made after approve by the Texas Director of Elections after appropriate review.

      Further, safeguards are needed to assure that only the approved update is installed on systems. The current practice potentially allows additional software to be installed under the guise that it is part of the operating system update.

[1] This checklist is identified on the NIST website but was published by the Center for Internet Security and is titled, "Windows 2000 Professional Operating System Level 2 Benchmark Consensus Baseline Security Settings", Version 2.2.1, November 15, 2004.

To assure a secure election system there should never be a point at which individuals from a single organization can change software. At a minimum individuals from two different organizations should approve and verify any changes to the operating system. In the case of operating system upgrades it would be preferable that the vendor recommend and the Director of Elections approve any patches to the operating system. Then that the vendor install the patches and the local jurisdiction have the tools and information to verify that the system delivered to them have only certified software, including the version and updates to the operating system. Further local jurisdictions should have the tools and information to confirm that no additional software has been added to the system

5. Recommended administrative use procedures for this system are needed.

Contents

Candidate System

This examination was convened to qualify the Hart InterCivic version 6.2.1 Voting System. The Hart InterCivic versions 3.3, 5.0 and 6.1 Voting System were previously certified for use in Texas and has been in use in a number of counties in the state and elsewhere in the country. While this examination looks at all aspects of the system particular attention was given to the changes from previously certified systems.

The information on system configuration in this test report is partially derived from and depended up on information contained in the ITA Qualification Test Report, Revision 3, for the Hart InterCivic 6.2.1 Voting System, dated August 11, 2006.

System Configuration

Hart InterCivic Voting System, version 6.2.1

NASED Certification # N-1-04-22-22-006 (2002)

System Components		
Unit/Application	**Version**	**Function**
Ballot Now™	3.3.11	Ballot printing on demand & CVR imaging
Rally™	2.3.7	Ballot accumulation
System for Election Records and Verification of Operations (SERVO™)	4.2.10	Election records and recount management
Judges Booth Controller™ (JBC)	4.3.1	Precinct controller for eSlate/DAU's
eScan™	1.3.14	Ballot scanner
Ballot Origination Software System™ (BOSS)	4.3.13	Ballot Preparation
Tally™	4.3.10	Tabulation
eCM Manager™	1.1.7	Security management
eSlate®/Disability Access Unit™ (DAU)	4.2.13	Electronic voting devices
Verified Ballot Option™ (VBO)		VVPAT device
Mobile Ballot Box™ (MBB)		Flash memory card

Previous Texas Certifications

The following table lists previous versions of the Hart InterCivic Voting System certified for use in Texas:

Description	Voting System Component	Version	Certification Date	Decertification Date
Hart Voting System 6.1	BOSS	4.2.13	8/9/2006	Certification Active
	Ballot Now	3.2.4		
	Rally	2.2.4		
	Tally	4.2.8		
	eCM	1.1.7		
	SERVO	4.1.6		
	JBC	4.1.3		
	eSlate	4.1.3		
	eScan	1.2.0		
Hart Voting System 5.0	BOSS	4.1.9	10/20/2005	10/1/2007
	Ballot Now	3.1.10		
	Rally	2.1.4		
	Tally	4.1.4		
	eCM	1.0.7		
	SERVO	4.0.13		
	JBC	3.1.3		
	eSlate	3.1.3		
	eScan	1.0.10		
Hart Voting System 3.3	BOSS	3.4.0	7/27/2004	10/1/2007
	Ballot Now	2.3.0		
	Rally	1.2.0		
	Tally	3.2.0		
	JBC	2.2.1		
	eSlate	2.0.13		

Functional Changes from Hart InterCivic 6.1 to 6.2.1

Changes from Version 6.1 to 6.2.1		
#	**Change**	**ITA Test Method**
Ballot Origination Software System™ (BOSS)		
1	Added support for Fractional Cumulative voting.	
2	Added interface to turn on/off Ballot Key on VBO print-out.	
3	Added interface to turn on/off the ability to print the write-in report for Election Day voting.	
4	Added translation file support for the eScan system.	
5	Added configuration settings for eScan/JBC to report precincts/splits consolidated on Tally tapes.	
6	Fixed defect that caused Vietnamese to be added instead of English for static audio in rare cases.	
7	Updated Card reader interface to work with new card reader.	
Ballot Now		
1	Enhanced ballot scanning processing to accept ballots in any orientation and ballot order with-in a batch.	
2	Added ability to accept orphan ballot sheets.	
3	Enhanced dependent contest support to allow for parent/child contests to span ballot pages on the same ballot sheet.	
4	Fixed defect for incorrect precinct Id in barcode during ballot printing (CR #6374).	
5	Added the full database path in the main form title (CR #4235).	
eCM Manager		
1	NONE	
eSlate System		
1	Enhanced Tally write-in report to include provisional totals and remove 100 contest with-in a precinct limitation.	
2	Added support to allow for consolidation of precinct/splits on Tally tapes.	
3	Added ballot count by party for primary elections.	
4	Added enhancements to Curb Side voting to allow for the eSlate to be plugged back into the system if	

	the access code was not entered before removal.
5	**Added ballot count summaries to the Tally tape.**
6	**Added the requirement to enter the administration password to close the polls to early on Election Day.**
7	**Added support to turn off following Day Light savings time.**
8	**Updated the JBC firmware to fix a defect found in the JBC tally report for a primary election when the configuration was set to combine splits. This defect was identified during certification testing.**
eScan	
1	**Added multiple language support. The eScan now supports all languages support by the Hart voting system.**
2	**Added multiple page ballot support.**
3	**Improved reliability of the scanner interface to eliminate system alerts.**
4	**Updated to remove defect that caused a system alert if long ballots we pulled out while being scanned.**
5	**Fixed defect that caused a system error when candidate names were longer than 30 characters without a space.**
6	**Added support to allow for consolidation of precinct/splits on Tally tapes.**
7	**Added ballot count by party for primary elections.**
8	**Improved ballot error screens presented to voters.**
9	**Fixed defect in bar code decoding algorithm that caused ballot with stub, that still had the separator line attached, not to be able to be decoded.**
Rally	
1	**Updated to link with new Tally interface to support new Fractional Cumulative voting.**
Tally	
1	**Support for Fractional Cumulative Voting.**
2	**Added support for multiple eScan sheet ballots.**
3	**Rewrite of the Canvass report to support up to 255 candidates.**
4	**Added the ability to export register voter totals.**

5	Added a blank ballot report by precinct.
SERVO	
1	Added support to turn on/off daylight savings time for a device
2	Support for printing multiple sheet eScan ballots.

Compliance Checklist

Vendor: Hart InterCivic	**Voting System: Hart Version 6.2.1**	
Pre-Test Requirements		
• Is Form 100 complete and satisfactory?	Yes ☒	No ☐
• If not satisfactory, please list questions to ask vendor.	Yes ☒	No ☐
• Review Form 100 - Schedule A - Have recommendations/issues made from previous exams been corrected or addressed?	Yes ☒	No ☐
• Review Form 101 - Are responses satisfactory?	Yes ☒	No ☐
• Review change logs and provide information for testing or questioning vendor	Yes ☒	No ☐
• Training manuals appear complete?	Yes ☒	No ☐
• Training manuals appear to be easy to use?	Yes ☒	No ☐
• Check with other jurisdictions where system is in use and ask questions regarding system, support and training.	Yes ☒	No ☐
• Did the system receive favorable reviews? If not, please explain.	Yes ☒	No ☐
• Do all configurations listed in application seem feasible? Keep this in mind during the examination to make sure components necessary to ensure the security are included in all configurations and that the configurations will meet the counties needs (scanner used as central and/or precinct, etc..)	Yes ☒	No ☐
• Vendors' proposals shall state a clear, unequivocal commitment that the election management and voter tabulation software user's application password is separate from and in addition to any other operating system password.	Yes ☒	No ☐
• Vendor's system shall support automated application password expiration at intervals specified by a central system administrator.	Yes ☒	No ☐
• Vendor shall discuss the steps required by the system administrator to implement and maintain automated password expiration. This discussion will include narrative concerning the degree to which the application password expiration capabilities are based on (a) the server or client's operating system, (b) the software application, or (c) both	Yes ☒	No ☐
• The vendor's proposal shall state the name of any automated incident, issue, or problem tracking system used by the firm in providing support to its election system clients. *(Note: Technical Bulletins for the previous year were provided and approved.)*	Yes ☒	No ☐
Verify Installation		
• Verify/List all hardware	Yes ☒	No ☐
• Verify/List all COTS hardware/software versions	Yes	No

	☒	☐
• Is the COTS hardware being demonstrated the same version as what was tested at the ITA?	Yes ☒	No ☐
• Is the COTS software being demonstrated the same version as what was tested at the ITA?	Yes ☒	No ☐
• Witness or actual install the software and firmware with the SOS CDs received from ITA.	Yes ☒	No ☐

Vendor: Hart InterCivic		**Voting System: Hart Version 6.2.1**		
Texas Law	**Federal Law**			
		System Review		
TEC 122.001		• Preserves the secrecy of the ballot	Yes ☒	No ☐
TEC 122.001		• Is suitable for the purpose for which it is intended	Yes ☒	No ☐
TEC 122.001		• Operates safely, efficiently, and accurately and complies with the error rate standards of the voting system standards adopted by the FEC (EAC)	Yes ☒	No ☐
TEC 122.001		• Is safe from fraudulent or unauthorized manipulation (physical exam and review of manuals)	Yes ☒	No ☐
TEC 122.001		• Permits voting on all offices and measures to be voted on at the election	Yes ☒	No ☐
TEC 122.001	HAVA	• Warns of Overvote - Prevents counting votes on offices and measures on which the voter is not entitled to vote	Yes ☒	No ☐
	HAVA	• Warns of Undervote	Yes ☒	No ☐
TEC 122.001		• Prevents counting votes by the same voter for more than one candidate for the same office or, in elections in which a voter is entitled to vote for more than one candidate for the same office, prevents counting votes for more than the number of candidates for which the voter is entitled to vote	Yes ☒	No ☐
TEC 122.001		• Prevents counting a vote on the same office or measure more than once	Yes ☒	No ☐
TEC 122.001		• Permits write-in voting	Yes ☒	No ☐
TEC 122.001		• Is capable of permitting straight-party voting	Yes ☒	No ☐
TEC 65.007		• Is capable of cross-over votes	Yes ☒	No ☐
TEC 122.001	HAVA	• Is capable of providing records from which the operation of the voting system may be audited	Yes ☒	No ☐
		• Is it easy to choose the appropriate ballot style?	Yes ☒	No ☐
		• Is the number of ballot styles available on a unit limited?	Yes	No

			☒	☐
		• Can you cancel the marking of a ballot after starting? Explain how.	Yes ☒	No ☐
		• Is there a way to properly secure all ports on the system?	Yes ☒	No ☐
		• Are instructions provided in the documentation for securing the system?	Yes ☒	No ☐
		• Usable for curbside voting?	Yes ☒	No ☐
		• How to setup or modify audio files	Yes ☒	No ☐
		• How to adjust volume	Yes ☒	No ☐
		• Does the system have any RF (Radio Frequency) communications?	Yes ☐	No ☒
		• Have representatives of the visually impaired community evaluated the accessibility of the system?	Yes ☒	No ☐
		• Test both early voting and election day - all functions opening/closing	Yes ☒	No ☐
		• Does system include sip 'n puff for accessibility	Yes ☒	No ☐
		• Does system include paddles for accessibility	Yes ☒	No ☐
		DRE Review		
TEC 122.001		• Preserves the secrecy of the ballot	Yes ☒	No ☐
TEC 122.001		• Is suitable for the purpose for which it is intended	Yes ☒	No ☐
TEC 122.001		• Operates safely, efficiently, and accurately and complies with the error rate standards of the voting system standards adopted by the FEC (EAC)	Yes ☒	No ☐
TEC 122.001		• Is safe from fraudulent or unauthorized manipulation (physical exam and review of manuals)	Yes ☒	No ☐
TEC 122.001		• Permits voting on all offices and measures to be voted on at the election	Yes ☒	No ☐
TEC 122.001	HAVA	• Warns of Overvote - Prevents counting votes on offices and measures on which the voter is not entitled to vote	Yes ☒	No ☐
	HAVA	• Warns of Undervote	Yes ☒	No ☐
TEC 122.001		• Prevents counting votes by the same voter for more than one candidate for the same office or, in elections in which a voter is entitled to vote for more than one candidate for the same office, prevents counting votes for more than the number of candidates for which the voter is entitled to vote	Yes ☒	No ☐
TEC 122.001		• Prevents counting a vote on the same office or measure more than once	Yes ☒	No ☐
TEC 122.001		• Permits write-in voting	Yes ☒	No ☐

TEC 122.001		• Is capable of permitting straight-party voting	Yes ☒	No ☐
TEC 65.007		• Is capable of cross-over votes	Yes ☒	No ☐
TEC 122.001	HAVA	• Is capable of providing records from which the operation of the voting system may be audited	Yes ☒	No ☐
		• Reports available by precinct?	Yes ☒	No ☐
		• In order to perform a manual recount, can you print cast vote records for a precinct (including early voting, ED and absentee?) from an individual DRE?	Yes ☒	No ☐
TAC 81.176		• A DRE must have the capability to segregate provisional votes from regularly-cast votes on the precinct returns	Yes ☒	No ☐
TAC 81.176		• The precinct returns must indicate the number of provisional ballots cast but not include actual provisional votes in the unofficial totals from the precinct	Yes ☒	No ☐
TAC 81.176		• Must provide a method for the cast provisional ballots to be accepted & added to the election results	Yes ☒	No ☐
		• Must be designed to not accept provisional write-in votes until the provisional vote has been accepted/approved.	Yes ☒	No ☐
TEC 122.033		• Equipped with a security system capable of preventing operation of the machine	Yes ☒	No ☐
TEC 122.033		• Equipped with registering counters that can be secured against access	Yes ☒	No ☐
TEC 122.033		• Equipped with a public counter	Yes ☒	No ☐
TEC 122.033		• Equipped with a private counter	Yes ☒	No ☐
TEC 127.154		• Does each unit have a permanent identification number?	Yes ☒	No ☐
		• Capability to have more than one ballot style available on a machine (used for consolidated precincts and early voting)	Yes ☒	No ☐
		• Can you easily choose the ballot style used on a DRE?	Yes ☒	No ☐
	HAVA	• Provide voters with disabilities the same opportunity for access & participation (including privacy & independence)	Yes ☒	No ☐
		• Usability of taking system to curbside voter	Yes ☒	No ☐
	HAVA	• Allow voter to review selections before casting ballot	Yes ☒	No ☐
	HAVA	• Allow voter to change selections before casting a final vote	Yes ☒	No ☐
		• Do multiple choice selections appear on summary screen? EX: vote for 2 or more	Yes ☒	No ☐
		• Does the system have any RF (Radio Frequency) communications?	Yes ☐	No ☒
		• Is there a way to properly secure all ports on the system?	Yes ☒	No ☐
		• Are instructions provided in the documentation for securing the system?	Yes	No

			☒	☐
		• Have representatives of the visually impaired community evaluated the accessibility of the system?	Yes ☒	No ☐
		• Test both early voting and election day - all functions opening/closing	Yes ☒	No ☐
		• Does system include sip 'n puff for low mobility	Yes ☒	No ☐
VVPAT Review				
TEC 122.001		• Preserves the secrecy of the ballot	Yes ☒	No ☐
TEC 122.001		• Is suitable for the purpose for which it is intended	Yes ☒	No ☐
TEC 122.001		• Operates safely, efficiently, and accurately and complies with the error rate standards of the voting system standards adopted by the FEC (EAC)	Yes ☒	No ☐
TEC 122.001		• Is safe from fraudulent or unauthorized manipulation (physical exam and review of manuals)	Yes ☒	No ☐
TEC 122.001	HAVA	• Is capable of providing records from which the operation of the voting system may be audited	Yes ☒	No ☐
		• The system shall permit the voter to correct any discrepancy between the electronic vote (summary screen) and the paper record before the vote is cast.	Yes ☒	No ☐
		• Is a paper record of each individual vote cast generated?	Yes ☒	No ☐
		• Is the paper record maintained in a secure fashion?	Yes ☒	No ☐
		• Has all items printed that would be needed to use as a manual count of the votes cast?	Yes ☒	No ☐
		• The paper printout includes notice if the printout has been voided by the voter?	Yes ☒	No ☐
		• Does the VVPAT print out have headers with precinct information that would allow a precinct by precinct recount?	Yes ☒	No ☐
Texas Real-time Audit Log Review				
TEC 81.62		• A central tabulating device must include a continuous feed printer dedicated to a real-time audit log, which prints out all significant election events and their date and time stamps. See VVSG 2005: 2.2.5.2.1.d: "The audit record shall be active whenever the system is in an operating mode. This record shall be available at all times, though it need not be continually visible." 2.2.5.2.1.g: "The system shall be capable of printing a copy of the audit record."	Yes ☒	No ☐
TEC		• Log error messages and operator response to those messages	Yes	No

81.62		See VVSG 2005 Section 2.2.5.2.2.a & 4.4.3.d	☒	☐
TEC 81.62		• Log the number of ballots read for a given precinct See VVSG 2005 Section 4.4.4.a & c & e	Yes ☒	No ☐
TEC 81.62		• Log completion of reading ballots for a given precinct See VVSG 2005 Section 4.4.3.b.3	Yes ☒	No ☐
TEC 81.62		• Log the identity of the input ports used for modem transfers from precincts See VVSG 2005 Section 4.4.2.g.1-4	Yes ☒	No ☐
TEC 81.62		• Log users logging in and out from election system See VVSG 2005 4.4.3.a.4, 4.4.3.d, 6.5.5.a & c	Yes ☒	No ☐
TEC 81.62		• Log precincts being zeroed See VVSG 2005 4.4.3.b.2	Yes ☒	No ☐
TEC 81.62		• Log reports being generated See VVSG 2005 4.4.3.d	Yes ☒	No ☐
TEC 81.62		• Log diagnostics of any type being run See VVSG 2005 4.4.2.a & d	Yes ☒	No ☐
		• Print any attempt to tally or load votes that have already been tallied or counted, identifying the precinct or source of the votes and flagging it as a duplicate	Yes ☒	No ☐
		• Print starting the tally software (e.g. from the operating system) or exiting the tally software, or any access to the operating system.	Yes ☒	No ☐
		• Record if a printer is paused, turned off, turned on, disconnected, and when reconnected.	Yes ☒	No ☐
Optical Scan System Review				
TEC 122.001		• Preserves the secrecy of the ballot	Yes ☒	No ☐
TEC 122.001		• Is suitable for the purpose for which it is intended	Yes ☒	No ☐
TEC 122.001		• Operates safely, efficiently, and accurately and complies with the error rate standards of the voting system standards adopted by the FEC (EAC)	Yes ☒	No ☐
TEC 122.001		• Is safe from fraudulent or unauthorized manipulation (physical exam and review of manuals)	Yes ☒	No ☐
TEC 122.001		• Permits voting on all offices and measures to be voted on at the election	Yes ☒	No ☐
TEC 122.001	HAVA	• Warns of Overvote - Prevents counting votes on offices and measures on which the voter is not entitled to vote	Yes ☒	No ☐
	HAVA	• Warns of Undervote	Yes ☒	No ☐
TEC		• Prevents counting votes by the same voter for more than one candidate	Yes	No

122.001			for the same office or, in elections in which a voter is entitled to vote for more than one candidate for the same office, prevents counting votes for more than the number of candidates for which the voter is entitled to vote	☒	☐
TEC 122.001		•	Prevents counting a vote on the same office or measure more than once	Yes ☒	No ☐
TEC 122.001		•	Permits write-in voting	Yes ☒	No ☐
TEC 122.001		•	Is capable of permitting straight-party voting	Yes ☒	No ☐
TEC 65.007		•	Is capable of cross-over votes	Yes ☒	No ☐
TEC 122.001	HAVA	•	Is capable of providing records from which the operation of the voting system may be audited	Yes ☒	No ☐
		•	Reports available by precinct?	Yes ☒	No ☐
		•	In order to perform a manual recount, can you print cast vote records for a precinct (including early voting, ED and absentee?) from an individual DRE?	Yes ☒	No ☐
TEC 127.154		•	Does each unit have a permanent identification number?	Yes ☒	No ☐
		•	Is there a way to properly secure all ports on the system?	Yes ☒	No ☐
		•	Are instructions provided in the documentation for securing the system?	Yes ☒	No ☐

Additional Examiner Notes

The following items were noted as part of this examination. In some cases administrative procedures can adequately protect a potential vulnerability in the system. However, in future versions of the system it would be preferable that the security vulnerabilities be mitigated.

In other cases these notes identify items of interest or observations of possible efficiencies that do not rise to a level to prevent certification.

1. There has been criticism of the Hart system in that when critical changes are made, such as using the administrative privileges to change vote totals, such events are not reported forward with the vote totals. The criticism has been that normal auditing practice is that changes of this nature are always highlighted with the old and new values being carried forward supported by appropriate notes.

   Future versions of the system should carry forward critical events, such as manual changing of vote totals, with the appropriate reports so that they are immediately brought to the attention of election officials. Such reports should continue to be listed, as they are now, in the detailed audit logs.

2. There has been a criticism that the database passwords are stored on the disk and is easily accessible.

3. There has been a criticism that the USB token used has the same password throughout the country.

4. It has been reported in reviews of this system in other states that it is possible to bypass the Hart software security settings. This item was discussed in the California evaluation of the Hart 6.2.1 system.

5. The possibility of a buffer overflow attack being executed against SERVO using eScan should be remedied in future versions of the system.

6. The California report states:

   “Some of the findings from previous studies on precinct count optical scanners were replicated on the eScan, and they allowed the Red Team to maliciously alter vote totals with the potential to affect the outcome of an election. These attacks were low-tech and required tools that could be found in a typical office.”

Reports of this type raise concerns about the system and should be addressed.

Annex A – Operating System Configuration

Operating systems have many configuration options and depending on the options selected can range from relatively secure to very vulnerable. For this reason the VSS 2002 and the VVSG 2005 require that the vendor specify the operating system configuration and that the security of the recommended by evaluated by the ITA, now VSTL.

The configuration of the operating system is a critical element to the overall system security. If the configuration of the operating system is not controlled many other security safeguards are of little value. The configuration of the operating system is a foundational piece essential to the overall security of the operating system. This fact is recognized and results in multiple requirements in the VSS 2002.

This annex is provided to support the recommendation that an operating system configuration be submitted by Hart InterCivic for review and approval.

Role of the Operating System

Typically voting systems are architected to rely on COTS operating systems such as Microsoft Windows®. An operating system is the computer software that controls the computer resources and provides the interface to access the computer resources. Key tasks of the operating system include process management, memory management, disk and file system control, and networking. Since the operating system has access to these key tasks, the security of the applications running on these operating systems rely on the security of the underlying operating system. The voting system software is a trusted application that calls on the operating system to perform these functions. This dependence makes the operating system a critical part of the voting system and its security is central to the security of the total voting system.

Operating System Security

Many commercially available operating system have undergone independent evaluation under the Common Criteria evaluation scheme to the EAL4 (Methodically designed, tested, and reviewed) level. These systems include HP-UX, IBM's AIX, IBM's z/OS, Microsoft's Windows 2003, Microsoft's Windows XP, Oracle's LINUX, Red Hat's LINUX, Sun Microsystems' Solaris, SUSE LINUX.

Operating System Security Threats

Although operating systems are evaluated under the Common Criteria and provide a solid foundation for security, there are many threats to operating systems ranging from trojans horses to remotely or locally launched service exploits. Operating system security can be weakened by misconfigurations, poor system maintenance, or poor site security.

Methods for Improving Operating System Security

A variety of methods are available for evaluating or improving operating system security. Some of the more common techniques are:

System Lockdown: Operating systems have the ability to provide data and process protection to users and applications. However, because these systems are intended for a wide variety of uses, many of the restrictive security controls are not enabled by default. Furthermore, it is often a difficult process for experience system administrators to apply appropriate settings to ensure security within their system. This process is referred to as "system lockdown" or "system hardening."

Rootkit Analysis: A rootkit is a program that takes control of the underlying operating system in an unauthorized manner. Becaused of their unauthorized nature, rootkits hide their presence from authorized administrators by hiding system files and data or concealing themselves from monitoring programs. Rootkit detection can be accomplished through active scanning for known rootkit binaries, through pre-installation checks on the software.

System Forensics: Many tools and techniques are available to investigate the digital states and past events within computer systems. This processed is often called computer system forensics. System forensics may investigate the current state of the system, contents of file systems, and past or present evidence of tampering or unauthorized network connections.

Trace Analysis: Software exists to monitor the operation of other software. For example all read and write operations to election data files can be monitored during a mock election. If files are accessed by software modules other than those expected further investigation is warranted.

Evaluation Tools & Methods

The following technology and software are currently available, these are listed as examples and do not represent a complete list or a recommendation:

System Lockdown Checklists

The National Institute for Standards and Technology (NIST) and the National Security Agency (NSA) have industry recognized and current checklist for Microsoft Windows Operating System. While specific changes may be advisable or necessary to adapt these checklists to specific voting systems they provide a credible reference and starting point for a voting system's operating system configuration. Differences between a configuration allowed for a voting system and these checklists should be identified, evaluated independently from the vendor and understood as to the reason for the deviation.

Tools for Root Kit Analysis, System Forensics and System Integrity Checking

A number of tools exist to perform root kit analysis, system forensics and system integrity checking. These tools can be used to examine a disk while running from a separate operating system. For example, a PC may be booted and run from a LINUX CD or flashdrive. This method avoids any possibility of hidden software intervening with the examination. Other tools are intended to be run in parallel with the application, using the same operating system. The purpose and application of these tools is different and each has a role. In combination they provide the means to rigorously evaluate the security of the operating system.

Area	*Tool Name*	*Unix or Windows*	*Functions*	*Licensing*
Rootkit Detection	Chkrootkit	UNIX	Rootkit detection	Permissible copyright[2]
	OSSEC		Log analysis, integrity checking, Windows registry checking, rootkit detection	GNU GPL
	Sophos Anti-Rootkit	Windows	Rootkit detection	Freeware
	F-Secure Blacklight		Rootkit detection and removal	Freeware
	Radix Anti-Rootkit		Rootkit detection and removal	Freeware
	RootkitRevealer		Rootkit detection and removal	Freeware
System Forensics	FTimes	Both	Integrity monitoring of critical files System Forensics: preserve timestamps Compare capability	BSD

[2] Redistribution and modifications are permitted provided that copyright notice and restrictions are contained.

Requirements Evaluated

The following specific requirements are relevant to the operating system configuration:

1. **VSS 2002 Vol. 1 Sec. 6.2.1.1**
2. **VSS 2002 Vol. 1 Sec. 6.2.2**
3. **VSS 2002 Vol. 1 Sec. 2.2.5.3**
4. **VSS 2002 Vol. 1 Sec. 4.1.1**
5. **VSS 2002 Vol. 2 Sec. 3.5**

Text of Relevant Requirements

The text of the requirements from the VSS 2002 of interest in this issue:

1. **VSS 2002 Vol. 1 Sec. 6.2.1.1**

   "**6.2.1 Access Control Policy**

   The vendor shall specify the general features and capabilities of the access control policy recommended to provide effective voting system security.

   6.2.1.1 General Access Control Policy

   Although the jurisdiction in which the voting system is operated is responsible for determining the access policies applying to each election, the vendor shall provide a description of recommended policies for:

   a. Software access controls;
   b. Hardware access controls;
   c. Communications;
   d. Effective password management;
   e. Protection abilities of a particular operating system;
   f. General characteristics of supervisory access privileges;
   g. Segregation of duties; and
   h. Any additional relevant characteristics. "

2. **VSS 2002 Vol. 1 Sec. 6.2.2**

   "**6.2.2 Access Control Measures**

   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;
b. Program unit ownership and other regional boundaries;
c. One-end or two-end port protection devices;
d. Security kernels;
e. Computer-generated password keys;
f. Special protocols;
g. Message encryption; and
h. Controlled access security.

Vendors also shall define and provide a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself."

3. **VSS 2002 Vol. 1 Sec. 2.2.5.3**

"**2.2.5.3 COTS General Purpose Computer System Requirements**

Further requirements must be applied to COTS operating systems to ensure completeness and integrity of audit data for election software. These operating systems are capable of executing multiple application programs simultaneously. These systems include both servers and workstations (or "PCs"), including the many varieties of UNIX and Linux, and those offered by Microsoft and Apple. Election software running on these COTS systems is vulnerable to unintended effects from other user sessions, applications, and utilities, executing on the same platform at the same time as the election software.

"Simultaneous processes" of concern include unauthorized network connections, unplanned user logins, and unintended execution or termination of operating system processes. An unauthorized network connection or unplanned user login can host unintended processes and user actions, such as the termination of operating system audit, the termination of election software processes, or the deletion of election software audit and logging data. The execution of an operating system process could be a full system scan at a time when that process would adversely affect the election software processes. Operating system processes improperly terminated could be system audit or malicious code detection.

To counter these vulnerabilities, three operating system protections are required on all such systems on which election software is hosted. First,

authentication shall be configured on the local terminal (display screen and keyboard) and on all external connection devices ("network cards" and "ports"). This ensures that only authorized and identified users affect the system while election software is running.

Second, operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object. This ensures the accuracy and completeness of election data stored on the system. It also ensures the existence of an audit record of any person or process altering or deleting system data or election data.

Third, the system shall be configured to execute only intended and necessary processes during the execution of election software. The system shall also be configured to halt election software processes upon the termination of any critical system process (such as system audit) during the execution of election software."

4. **VSS 2002 Vol. 1 Sec. 4.1.1**

"**4.1.1 Software Sources**

The requirements of this section apply generally to all software used in voting systems, including:

- Software provided by the voting system vendor and its component suppliers;
- Software furnished by an external provider (for example, providers of COTS operating systems and web browsers) where the software may be used in any way during voting system operation; and
- Software developed by the voting jurisdiction.

Compliance with the requirements of the software standards is assessed by several formal tests, including code examination. Unmodified software is not subject to code examination; however, source code generated by a package and embedded in software modules for compilation or interpretation shall be provided in human readable form to the ITA. The ITA may inspect source code units to determine testing requirements or to verify that the code is unmodified and that the default configuration options have not been changed.

Configuration of software, both operating systems and applications, is critical to proper system functioning. Correct test design and sufficient test execution must account for the intended and proper configuration of all system

components. Therefore, the vendors shall submit to the ITA, in the TDP, a record of all user selections made during software installation. The vendor shall also submit a record of all configuration changes made to the software following its installation. The ITA shall confirm the propriety and correctness of these user selections and configuration changes."

5. **VSS 2002 Vol. 2 Sec. 3.5**

   "**3.5 Functionality Testing for Systems that Operate on Personal Computers**

   For systems intended to use non-standard voting devices, such as a personal computer, provided by the local jurisdiction, ITAs shall conduct functionality tests using hardware provided by the vendor that meets the minimum configuration specifications defined by the vendor.

   Volume II, Section 4, provides additional information on hardware to be used to conduct functionality testing of such voting devices, as well as hardware to be used to conduct security testing and other forms of testing."

Annex B – Delivery and Verification of Software and Firmware

File Signatures – Hart InterCivic Version 6.2.1

Chain of Custody

The software and firmware for the system was requested from the ITA (Independent Testing Authority) and delivered directly from them. The software and firmware was sent on a CD. The representatives of Hart InterCivic verified that the software delivered from the ITA was the software they had submitted for certification. This procedure provided a vendor independent delivery of the NASED certified software and firmware.

The build environment

The VSG 2002 standard requires the ITA to supervise a witness build of the code to be used. A clear record of the executable files produced by the build is necessary. This would certainly include the recording of the digital signatures of all executable files produced. The EAC has incorporated these elements into its certification system and it may be expected that future state certifications will have the added benefit of these protective measures.

The software and firmware used in the Hart InterCivic version 6.2.1 system did have file signatures deposited with the NIST NSRL (National Institute of Standards and Technology National Software Reference Library).

File Signatures

The CD supplied from the ITA was used to install the software on the system at the beginning of the examination.

After the installation a self-booting CD, containing the Knoppix (Linux) operating system and the NARA software was used to check file signatures. The results were stored onto a USB drive, also provided by the examiner. Thus, the file signatures of the software and firmware examined for state certification were obtained. These file signatures were then be used to verify that the software and firmware installed for use is identical to that listed in the NIST NSRL database.

PC System Information

The system information utility provided with the windows operating system was used to obtain the configuration of the PC's supplied for the examination. The system configuration information was saved to a USB drive as a record of the systems submitted for certification.

State Certification & Pre or Post Election Verification

Using the file signatures obtained during the examination a local official performing pre or post election verification should be able to confirm that all software is valid and unmodified from its certified version. However, to do this requires tools that have yet to be fully developed, would be required. For the software resident on PC's the self-booting CD used in this exam with the addition of a signature comparison function would be necessary to confirm that the software loaded is identical to that certified. For voting stations and optical scanners their firmware would have to be verified before it is loaded and after that assured by the physical security and seals placed on the device.

Annex B –NASED Systems Certification

Company	Voting System	Software	Hardware/Firmware	System ID # / VSS Version	Final Report Date
Hart	InterCivic eSlate System Version 3.0	BOSS version 3.0.03.44 Ballot Now version 2.00.09 Rally version 1.1.13 Tally version 3.1.18.0 COTS software: MS Windows 2000 Professional, service Pack 4	Scanner = Kodak 1500D Scanner = Fujitsu M4099D Scanner = Fujitsu M4097D Scanner = Kodak 3520D Scanner = Kodak i840	N-1-04-12-12-001 (1990)	9/18/2003
Hart	InterCivic eSlate System Version 3.1	BOSS version 3.4.0 Ballot Now version 2.1.0 Rally version 1.2.0 Tally version 3.2. 0 Servo 2.0.10	Desktop workstation, Dell GX-1240, Ser. No. 956L111 Desktop workstation, Dell GX-1240, Ser. No. 746L111 JBC, Ser. No. C01026 Firmware Version 2.0.13 JBC, Ser. No. C01161 Firmware Version 2.0.13 eSlate3000 Ser. No. A04D10 Firmware Version 2.0.13 eSlate300	N-1-04-12-12-002 (1990)	12/19/2003
Hart	Hart InterCivic eSlate System Version 3.2	BOSS version 3.4.0 Ballot Now version 2.02.05	Desktop workstation, Dell GX-240 Ser. No. 956L111	N-1-04-12-12-003 (1990)	1/16/2004

		& 2.02.06	Desktop workstation, Dell GX-240 Ser. No. 746L111 MBB Card Reader Printer, HP DeskJet 932C PSINET Number A000265656		
Hart	Hart InterCivic eSlate System Version 3.3	BOSS version 3.4.0 Ballot Now version 2.3 Servo version 2.0.10 Rally version 1.2.0 Tally version 3.2.0	Desktop workstation, Dell GX-240 Ser. No. 956L111 Desktop workstation, Dell GX-240 Ser. No. 746L111 MBB Card Reader Printer, HP DeskJet 932C PSINET Number A000265656	N-1-04-12-12-004 (1990)	5/5/2004
Hart	Hart InterCivic eSlate System Version 3.4	BOSS version 3.5.4 Ballot Now version 2.3 Servo version 2.0.10 Rally version 1.2.0 Tally version 3.2.0	eSlate 3000 release 2.3.8 JBC1000 firmware revision 2.3.8	N-1-04-12-12-005 (1990)	8/2/2004
Hart	Hart InterCivic eSlate System Version 4.0	BOSS version 4.0.48 Ballot Now version 3.0.24 Rally version 2.0.11 Tally version 4.0.25 eCM Manager 1.0.7 Servo 3.0.17 COTS software: MS Windows 2000 Prof, Service Pack 4	JBC Firmware Version 3.0.15 eSlate Firmware Version 3.0.15	N-1-04-22-22-001 (2002)	3/31/2005

Hart	Hart InterCivic eSlate System Version 4.1	BOSS version 4.0.48 Ballot Now version 3.0.24 Rally version 2.0.11 Tally version 4.0.25 eCM Manager 1.0.7 Servo 3.0.17 COTS software: MS Windows 2000 Prof, Service Pack 4	JBC Firmware Version 3.1.2 eSlate Firmware Version 3.1.2	N-1-04-22-22-002 (2002)	5/18/2005
Hart	Hart InterCivic eSlate System Version 5.0	BOSS version 4.1.9 Ballot Now version 3.1.10 Rally version 2.1.4 Tally version 4.1.4 eCM Manager 1.0.7 Servo 4.0.13 BOSS Util 2.3.8 HartLib 1.1.5 COTS software: MS Windows 2000 Prof, Service Pack 4	JBC Firmware Version 3.1.3 eSlate Firmware Version 3.1.3 eScan Firmware Version 1.0.10	N-1-04-22-22-003 (2002)	10/14/2005
Hart	Hart InterCivic eSlate System Version 6.0	BOSS Ver. 4.2.13 Ballot Now Ver. 3.2.4 Rally Ver. 2.2.4 Tally Ver. 4.2.8 eCM Manager 1.1.7	JBC Firmware Ver. 4.0.19 eSlate Firmware Ver. 4.0.19 eScan Firmware Ver. 1.1.6 VBO Firmware Ver. 1.7.5	N-1-04-22-22-004 (2002)	3/6/2005

		Servo 4.1.6 Boss Util. 2.4.14 Hart Lib. 1.7	COTS Scanner Fujitsu M4099D COTS Printer HP LaserJet 2420D		
Hart	Hart InterCivic eSlate System Version 6.1	BOSS Ver. 4.2.13 Ballot Now Ver. 3.2.4 Rally Ver. 2.2.4 Tally Ver. 4.2.8 eCM Manager 1.1.7 Servo 4.1.6 Boss Util. 2.4.14 Hart Lib. 1.7	JBC Firmware Ver. 4.1.3 eSlate Firmware Ver. 4.1.3 eScan Firmware Ver. 1.2.0 VBO Firmware Ver. 1.7.5 COTS Scanner Fujitsu M4099D COTS Printer HP LaserJet 2420D	N-1-04-22-22-005 (2002)	3/3/2006
Hart	Hart InterCivic eSlate System Version 6.2.1	BOSS Ver. 4.3.13 Ballot Now Ver. 3.3.11 Rally Ver. 2.3.7 Tally Ver. 4.3.10 eCM Manager 1.1.7 Servo 4.2.10 Boss Util. 2.5.8 Hart Lib. 4.0 Translate DLL 1.8.2	JBC Firmware Ver. 4.3.1 eSlate Firmware Ver. 4.2.13 eScan Firmware Ver. 1.3.14 VBO Firmware Ver. 1.8.3 COTS Scanner Fujitsu M4099D COTS Scanner Fujitsu M4097 COTS Scanner Kodak i660 COTS Scanner Kodak 3520 COTS Scanner Kodak 1500 COTS Scanner Kodak i830 COTS Printer HP LaserJet 2420D	N-1-04-22-22-006 (2002)	8/7/2006