

California Secretary of State
Consultant's Report on:

ES&S, Inc.
InkaVote Precinct Ballot Counter

Including:
International Lottery and Totalizer Systems, Inc. InkaVote Precinct Ballot Counter
version 1.10
Unisyn Voting Solution's Election Management System version 1.1

Prepared February 24, 2006
By Steve Freeman

Scope of Work and Reporting

This report is prepared as a supplement and attachment to the "Staff Review and Analysis" (SOS Report) as prepared by the California Secretary of State's Office of Voting Systems Technology Assessment (OVSTA) on February 22, 2006.

A large part of the consulting work product was providing assistance to OVSTA in both the planning and conduct of voting system tests. The majority of the findings are reported in the SOS Report. This report will be limited to a description of the tasks performed and findings that are not covered in the SOS Report.

Our expertise is in methodologies for examining computerized voting systems, analysis of systems operation, developing measurements of system compliance with established criteria, identification and analysis of system anomalies and collecting evidence of system characteristics and compliance.

We are not attorneys and do not offer legal advice. We have assisted the California Secretary of State in the collection of facts and evidence that he will use in reaching certification decisions. However, to advise him on the determination of whether the system complies with California's certification requirements would require an interpretation of law. Accordingly, we do not provide recommendations or any opinion as to whether the system can be certified. Recommendations to the Secretary for or against certification are within the duties of the OVSTA and are included in their report.

The work that we have performed and our findings are strictly limited to the specific serial numbered hardware elements and specific software elements tested during the examination. An inventory of those items is included as attachment A to this report. The results described in this report should be reliable and repeatable for those specific items. The decision to apply those results to decisions about other items is solely at the discretion and risk of the Secretary of State and the purchasers of systems. Although attachment A of this report can be used as part of a baseline for reaching conclusions

about compliance of other items, users of this report who wish to arrive at such conclusions about compliance of purchased systems or the compliance of a system in use should conduct appropriate acceptance testing or system validation analysis to support those conclusions. If they do not have a high level of well-founded confidence in their ability to conduct acceptance testing or validation analysis, we strongly recommend that they contract for the assistance of someone with the required knowledge and experience.

References

1. [Unisyn 1.02] Cyber Draft Report, *Unisyn INKAVote Precinct Ballot Counter (PBC) Voting System Qualification Test Report, Report Version 1.2 Created 11/16/05 (EMS Version 1.02)*, 16 Nov 2005.
2. [ILTS 1.9.2] Wyle Report 51349-01, *Hardware Qualification Testing of the INKAVote Precinct Ballot Counter, Firmware Release 1.9.2*, February 7, 2005
3. [ILTS 1.10] Wyle Preliminary Report 53006-01, *Change Release Report of the ILTS InkaVote Precinct Ballot Counter (PBC) (Firmware Release 1.10)*. 20 Dec 2005.

Introduction

In compliance with California Elections Code 19200 and 19205, Election Systems & Software (ES&S) applied for certification of the InkaVote Plus system consisting of:

1. International Lottery and Totalizator Systems, Inc (ILTS) Inkavote Precinct Ballot Counter (PBC), 1.10. The InkaVote PBC is a marksense ballot reader and ballot box for the InkaVote Unisyn Vote optical-scan ballots. The PBC is programmed and configured for an election using the Election Loader application over a secure local area network. Voted InkaVote ballots are fed into the ballot slot one at a time. If configured for precinct use, the PBC will initially reject a ballot that is over voted in one or more contests and will print a slip for the voter detailing the errors on the ballot. The PBC can also be configured to provide similar warnings if any or all contests are under voted. When all the votes have been counted, the results are saved to the Transport Media (TM). The results are then uploaded from the TMs into the Unisyn EMS for tabulation and reporting.

The InkaVote PBC can also be configured to tabulate absentee ballots prior to and after Election Day. System security features prevent the system from reporting the results prior to the close of the polls on Election Day.

The PBC features an attached voting booth that allows audio voting for the visually disabled. Audio instruction is provided through a headset. A detachable 5-key keypad records the voter's choices. After the voter finalizes the ballot, the votes are printed on an InkaVote formatted slip of paper from the printer located in the booth. This slip of paper is inserted into the PBC and tabulated in the same manner as other ballots.

For security, the PBC runs on a Linux operating system and is designed to detect and shutdown the PBC if an invalid TM is inserted.

2. Unisyn Voting Solution's Election Management System (EMS), v 1.1. Includes:
 - a. Ballot Generator 1.1- In conjunction with the Database Setup utility the Ballot Generator allows the jurisdiction to: set up the database for district types, languages and political parties; define an election, including contests, candidates, precinct assignment; define ballot and generate ballot layout, including candidate rotation, audio ballot information and alternative language support. This data is exported to a single, encrypted XML file for use by the Election Converter.
 - b. Election Converter 1.1- The Election Converter allows the jurisdiction to combine actual audio voting files with the election information produced from the Ballot Generator. In addition, the configuration options for the PBC are set in this application. The Election Converter is used to create the export Election CD used to program the PBCs for an election.
 - c. Election Loader 1.1- The Election Loader uses the election CD produced in the Election Converter to program the PBCs over a local area network.
 - d. Vote Converter 1.1- The Vote Converter is used to upload vote results from each PBC into the database.
 - e. Central Tabulation 1.1- The Central Tabulator is used to monitor the progress of vote results collection, as well as to generate reports on the election. The application includes a set of non-customizable reports. For more complex reporting, a read-only account provides access to the database for reporting via a third-party report generation tool.
 - f. S.S.O. Report 1.1- Unisyn Voting Solutions Supplemental Statement of Votes Cast Report, Version 1.1.

Description

The EMS portion of the system is designed to allow maximum separation of function (a strong security/audit principle). The modules Ballot Generator; Election Converter; Election Loader; Vote Converter; and Central Tabulation are designed to work on separate computers with the election database only appearing where needed. (See Attachment A for a diagram of the split of functions in terms of distribution between test computers). The system uses a commercial SQL database package, MySQL, to manage the election definition and data. The design's Election and Vote Converters deserve special attention as they were intended to be an interface where election support from alternate election management systems may be used to program to and upload results from the PBC units. This certification test only confirmed the interface between the Unisyn EMS and the ILTS PBC.

The design includes an unusually varied assortment of transfer media and pathways (see diagram in attachment).

The ES&S InkaVote Voting System is designed to use the InkaVote ballot currently used in Los Angeles. This is based on former punch card style of ballot that has been redesigned to mark the ballot instead of using a pre-punched card. The card supports 312 voting positions. Instead of punching the card out, the recorder allows the voter to mark the voting position with an ink stamp device or with a pencil or pen.

The PBC, a Linux based system, reads, records, and stores the ballots and can provide precinct level tally reports, if needed. It is accompanied with an optional ADA booth that allows a visually disabled voter or a voter who cannot read to listen to audio instructions for completing the ballot (selection of voter's choices and marking the choice). The ADA Voting Booth is audio only. No visual display of the ballot is presented to the voter. Visually abled voters mark the ballot directly using a voting booklet (the same as used in other installations using the InkaVote ballot), which shows the contests, candidates or choices, and marking positions. The actual ballot does not have the contest or candidate information printed on the ballot, so the ballot must be coded and interpreted with the appropriate voting booklet or layout list for the correct precinct and ballot format.

NASED Qualifications/State Certifications

<u>Component</u>	<u>NASED #</u>	<u>State Certification</u>
1. InkaVote Voting System 1.1	Pending	new
2. InkaVote PBC 1.10	Pending	new

An earlier version was tested and certified by NASED in November. During state testing, additional changes were made and the changes were sent back to the Federal Independent Testing Authorities for updated reports. The final report is not expected until after this report is filed.

Findings

With the exception of specific findings highlighted below, the system generally performed to the level expected during testing. With appropriate operating procedures the system appears to be capable of being used to conduct elections producing accurate results meeting the functional requirements of state and federal law, with appropriate security and user friendly interfaces.

Exceptions where the system did not perform to the level expected were:

1. The system does not incorporate any devices for physically marking the InkaVote ballots. While such devices were employed and tested as part of the examination, the applicant had not represented these devices as part of the system in the application for certification. If this system is certified, it should be used without

such devices until a subsequent application that incorporates vote recorders is presented, tested and certified.

2. The PBC is designed to read the standard InkaVote ballot with or without the write-in stub attached. During testing, it was also discovered that the PBC will also accept a ballot with the stub that has a ballot serial number attached. This stub is normally detached and given to the voter prior to insertion of the ballot in the ballot box. Under California law, if the ballot is accepted with this unique identifier, the ballot must be discarded and not counted. Since the InkaVote PBC is designed for voters to insert the ballot themselves, this issue must be addressed in the system's Use Procedures. The vendor should modify the system to prevent ballots from being inserted with the serialized stub attached.
3. On the PBC units tested, there was no mechanism to physically secure and lock the network port. This must be addressed with a requirement in the official Use Procedures that this cap be sealed with a serialized tamper-evident seal. Future versions of the PBC should include a means of physically preventing access to this port, such as a locking door to cover the port.
4. It is possible to insert a ballot directly into the ballot box and bypass the PBC ballot reader. The vendor needs to ensure that production models of the PBC will include a foam gasket on the ballot box to prevent this.
5. The system could not support the California Supplemental Statement of Vote Cast (SSOV) reporting requirement. Unisyn developed a special add-on module to produce the report. When tested, the report did not handle DTS records correctly and had to be revised. A revision was sent to Ciber for source code review. Ciber provided the source code review, but had a member of our test team perform the trusted build as their agent and return it with documentation to update and complete the Ciber formal report for this release.
6. Software Loader is a utility for loading software onto the PBC. Its use simplifies, but is not essential to, loading the software. Due to the fact that it has not been submitted to the ITAs for review and testing, it has been excluded from this application for certification.
7. Transfer Media are USB memory devices that carry results from the precinct ballot counters to the Vote Converter and Tabulator applications. During the course of the test, there were several incidents where results could not be recovered from the Transfer Media. In order to remedy the problem, these Transfer Media need to be "purged" with a special program that is not a part of the package submitted for certification. During the volume testing, this could become a potential problem.
8. The secrecy sleeve for the ballot is too short and can expose votes. This is especially true for visually disabled voters, who cannot see what part of the ballot is exposed.
9. The ADA booth only supports those who require an audio ballot. There is no visual display of the ballot in that booth. The system does not provide a sip and puff interface.

10. The election definition is time sensitive. The definition includes times/dates for the polls opening and closing. On the day of the election, the PBC units must be powered up after the open time setting for the polls. Absentees ballots can not be counted on Election Day--they can be counted the days preceding election day and then finished the day after.
11. Early voting requires separate counts and is expected to require ADA support. The only current mode that allows separate accounts to be collected is the Absentee mode. Absentee does not allow ADA Booth operations (since Absentee voters would not use the booth). A procedural work around is needed to support ADA use with Early Voting operations.
12. Provisional ballots may be fed into the InkaVote Plus, but they are not counted. The InkaVote Plus only allows the ballot to be checked for user entry problems.

Security Observations

Microsoft and National Institute of Standards and Technology (NIST) have established a project to support the setup of Windows operating systems as a secure working environment. Part of that is a guide for creating a lock down setup checklist that reduces the vulnerabilities for applications by shutting down services and features that may be exploited to gain control or access to program resources. If a local ITA security manager wishes to tighten security by eliminating services or access, the checklist identifies the services and features that are required for proper operation and those that may be eliminated or restricted. We test with the checklist when we can get one to verify that the voting system can correctly operate under California rules with the minimal services and accesses. The Unisyn component has provided a security checklist for their applications and we successfully tested using it. In addition, we tested to what extent system administrator privileges are required to conduct an election and to what extent lesser privileged users are blocked from making, deleting or changing application files

Installation of the Trusted Build PBC programs was done by a utility Software Loader that was not part of the Federal or State certification package. This program is a warehouse/manufacturer level utility and is not considered as needed as a deliverable item. During installation of the trusted build, we could not easily validate that it was loading the witnessed build programs and not adding/modifying others. Both it and the Election Loader access the Software Verification program on the PBC unit to verify the correct files are installed. The process uses electronic hash signatures (MD5 hashes) to verify the current installed software and to identify what programs need to be replaced for the update. We used a manual procedure to duplicate the process for installing updates and checking versions installed. We discovered that some older files were still on the system, which caused a problem for the Software Loader since it did not detect a critical file was out of date or recognize programs which were no longer needed. The Software Loader also may be used to perform a simple verification that the correct version files are installed based on an encrypted CD copy. The errors in recognizing and deleting the

unnecessary programs and not recognizing another file that needed to be updated indicates more work is needed on this utility.

The Unisyn Windows workstations were setup to use Administrative and user level login accounts. Unisyn recommends strong passwords, but leaves the responsibility to the local jurisdiction to set controls on the password. As delivered, the system may support blank passwords. The application passwords are setup as MySQL passwords. MySQL passwords are 6-15 characters, with at least one non-numeric character and no special characters (including blanks). The simplest password is 'aaaaaa'. The system supports three levels of account: the SuperUser, Admin, and Maintenance, but does not use all three on every module of the system.

1. The SuperUser account is the only one that can add or change all levels of access accounts. In Election Converter, it is also needed to export an Election Definition to CD (an encrypted interface), re-open an Election, mark an Election as concluded, and delete an Election. The initial installation password for the SuperUser is a default which is used to initially open and setup the database but should be changed immediately and periodically after the initial setup. SuperUser Accounts are created in Ballot Generator or Election Converter. The SuperUser account is needed to save and delete elections. To change out of Admin account into SuperUser requires a full shut down and reboot of the system; no fast switching of login accounts is supported under the secure setup.
2. The Admin performs most functions in the EMS, including some account maintenance, but is not as extensive as SuperUser. Admin may view and change Admin and Maintenance Technician passwords.
3. The Maintenance Technician account is used by Election Loader, PBC Maintenance operations, and Vote Converter. Its password is a minimum of seven characters, upper/lower/numerical digit with at least one non-numerical and no special characters. Maintenance Technician accounts are added in the Election Converter.
4. Location passwords are not accounts but are used, optionally, to login to the InkaVote PBC by the pollworker.
5. With the exception of the Maintenance Password, all passwords are stored hashed.
6. When we went into final processing and reporting, we found the user accounts/passwords had been reset to default. The election database had been reloaded and automatically reset.
7. The PBC system is not normally accessible at the operating system (Linux) level except for installation of the application software and the election definition. At that time, the units are connected by a local TCP/IP network. Once the software/election is installed, the units should be disconnected from the LAN. The Linux is setup up with a Root and Maintenance password. The Root is not normally used but, in this case, it was necessary in order to complete the installation of the firmware and to verify the installed files. Passwords were defined as 7-12 characters, allowing mixed case and at least one non-numerical character (no special characters).
8. The SSOV Viewer uses a hard-coded user account 'Report' and requires SuperUser login. The password may be reset on entry to new password using the MySQL standard password restrictions. The Report account may be used to access the

Election Database directly and access values (extract data) for use in building reports, but does not provide any access privileges to modify or delete data. As designed, the final data in the database is not protected from anyone who can gain physical access to a copy of the election database. The SSOV Viewer simply provides additional support to select and format the data as an SSOV report.

We tested the security configuration setup and MySQL security by identifying and attempting to modify, delete or replace selected files used by the election programs. The setup blocked simple opportunities to alter the system. We also could not install other programs or change the secure setup. Under Windows Admin user accounts, the database files could not be changed or deleted.

As configured for the system being tested, the ballot box had a gap between the scanning unit and the box. It was possible to slip ballots into the ballot box from the side and no go circumvent detection by the scanner.

The internal partition of the ballot box which separates ballots processed as either provisional or counted is inadequate and allows ballots to slip under the partition and intermingle with ballots of the other type. A modification of ballot box should correct this problem.

The Vote Converter must have the Election CD (encrypted). The Election is not stored in dynamic random access memory. The CD is a critical component and provides a convenient way to secure the election definition, as it may be stored in safe.

Attachment A

Hardware Descriptions

Precinct Ballot Counter
Firmware Version 1.10
Serial Number UNI 240025
With:
ADA Booth
Serial Number UNI 00003

Precinct Ballot Counter
Firmware Version 1.10
Serial Number UNI 240024
With:
ADA Booth
Serial Number UNI 00016

Precinct Ballot Counter
Firmware Version 1.10
Serial Number UNI 240023
With:
ADA Booth
Serial Number UNI 00001

Precinct Ballot Counter
Firmware Version 1.10
Serial Number UNI 240026
With:
ADA Booth
Serial Number UNI 00011

Precinct Ballot Counter
Firmware Version 1.10
Serial Number UNI 240022
With:
ADA Booth
Serial Number UNI 00004

Compaq DS-MS/ Pro. MMC SM-XP
Serial # CNF545016V
With Software Loader 1.0

Epson Desktop PC
Serial # ENEV003873
With:
HP Laserjet 1300
Running:
Windows XP SP2
Ballot Generator v. 1.1
Vote Converter v. 1.1
Vote Tabulator v. 1.1

Epson Desktop PC
Serial # E312214367
With:
CD Writer TDK # 5201B
Serial # B523248U0028343
Running:
Windows XP SP2

Election Converter v. 1.1

Epson Desktop PC
Serial # ENEV003880
Running:
Windows XP SP2

Election Loader v. 1.1

Description of System Setup

Comments on diagram below:

The diagram shows the layout of equipment for loading election. The connection between EMS computers and PBC is a local area network. The network is disconnected for voting.

This configuration is used for election reporting (moving the results from PBC units to the vote tallying equipment via USB drive). We used USB Thumbdrives).

Connections in setup:

1. Database setup and Ballot Generator. In the initial design, these tasks were configured so the setup was done entirely by Unisyn service personnel using MySQL operations and was not part of the tested system. Although the setup task still exists, the setup and election database creation have been added to, and tested as, part of the security envelope of the Ballot Generator. As it may actually be used, the created election database may be imported from a separate unit.

2. Ballot Generator to Election Converter. The interface is through the Ballot XML file transfer. The source of the transfer data may be another EMS and not a Unisyn Ballot Generator, but this usage was not tested.
3. Election Converter to Election Loader. The interface is through an encrypted CD.
4. Election Loader to the PBC. As performed, the interface was through a temporary local network connection to a number of PBCs linked in the network. A related utility, the Software Program Loader, installs the PBC application software using the same concept but was not submitted and tested with this release (see later comments). The files are encrypted and signed to detect errors or modifications.
5. PBC to Vote Converter. The PBC uses USB portable drives and encrypted results files. In the tests, these consisted of specially formatted “thumb drives” but the terminology used in the specifications suggests that other USB memory devices may be used.
6. Vote Converter to Tabulator. The Vote Converter is expected to be co-resident with the Tabulator. The documentation identifies the transfer format as decrypted data files appropriate to the election database import operation. Although it was initially a copy of the election definition database, note that the Tabulator database may be a separate and protected copy.
7. Tabulator to the extra module for Supplemental Statement of Vote (SSOV). The SSOV module is a special report to meet California SSOV requirements and uses SQL queries on the MySQL database instances containing tabulated results.

Voting System Equipment Layout

