POPULEX Digital Paper Ballot Voting System
PopulexSlate with PPF, v. 9.21-C
Populex EMS software, v. 3.05

STAFF REVIEW

Executive Summary

Secretary of State staff and the State's technical consultants went to the Populex headquarters in Elgin, Illinois during the week of May 22, 2006, to perform State certification testing on the Populex voting system.

Shortly after arrival, we discovered that federal end-to-end testing had not been completed on the version of the system that had been proposed for certification in California. Further, previously identified issues regarding system configuration had not been fully resolved and a trusted install version of the software was not yet available from the federal Independent Testing Authority (ITA).

As a courtesy to the vendor, Secretary of State staff and consultants remained on site for two days to review the system in order to provide a preliminary appraisal to the vendor and to identify any potentially serious issues with the system that should be corrected before State testing of the system formally begins. This report details the findings of that review.

Reviewers found many problems with the system as presented, some of which will be deemed fatal and will prohibit approval of the system if not corrected. These defects include a complete lack of support for ballot rotation, including an inability to report vote results for rotated contests without manual aggregation and tabulation of the vote tally for those contests. Similarly, the system cannot report the canvass with the level of detail required to be provided in the Supplement to the Statement of Vote.

There were also severe security concerns with this system that cannot be readily resolved without design modifications.

Finally, the sheer number of less severe issues identified, together with the fatal problems and security concerns discussed above, suggest this is a system that is not ready or appropriate for use in California, except possibly in the smallest of jurisdictions and under extremely limited circumstances. Given the scope of issues found, it is questionable whether this system can be appropriately modified and passed the complete Federal and State certification processes in time for use in the November 7, 2006 General Election.

1. Introduction

On May 22, 2006, Secretary of State staff and the State's technical consultants, Steve Freeman and Paul Craft, arrived at Populex Corporation headquarters in Elgin, Illinois.

We were there to perform the State examination and testing of the Populex voting system proposed for use in California.

After a brief meeting with Populex staff and a high-level demonstration of the system, it was determined that actual testing of the system could not take place because a trusted install of the application software and firmware was not available. In fact, the version of the system proposed for use in California had not yet completed end-to-end testing with the federal ITAs.

Although it was not possible to perform the certification examination and testing of the system at that time, Secretary of State staff and the consultants did spend two days reviewing the system in greater detail, attempting to identify any major concerns with this voting system that might be correctable before Populex resubmits the system for certification. It was clearly communicated to the vendor that this review was by no means exhaustive, and that it was entirely possible that significant, and possibly fatal, new issues could be discovered in subsequent testing of the system.

This report highlights the most significant of our findings from that two-day review. This report is meant as an aid a) to counties who have not yet committed to a HAVA-compliant voting system and are considering their options, and b) to the vendor, Populex, to assist in preparation for possible subsequent California testing.

2. System Description

The proposed Populex System has two main components: The PopulexSlate device and the Election Management System (EMS) software application. Both are discussed in detail below, as well as the Populex ballots that are integral to this system.

It should be noted that this system does not support absentee or other mail ballots. Jurisdictions using this system would need to use another voting system to support the absentee and mail-ballot precincts in an election, and would have to find a mechanism to aggregate and report the vote results from each system.

2.1. PopulexSlate with Polling Place Functions software application (PPF), version 9.21-C

The PopulexSlate is a versatile device for the polling place that can be set to serve one or more of the following roles:

- Judge's Check-In Station – to program voter election keys (smart cards) with the correct ballot style for each voter;
- Voting Station – for voters to actually cast and print their ballots;
- Personal Verification Station – for voters to independently verify their ballots before they are tabulated and/or deposited into the ballot boxes; and
- Ballot Counting Station – to read and tabulate ballots either throughout the day or upon the close of the polls.

As noted above, a PopulexSlate can be configured to serve multiple roles at the same time. For example, it can be configured to be both a Judge's Check-In Station and a Ballot Counting Station, or it can be configured to be both a Voting Station and Personal Verification Station. The PopulexSlate also provides redundancy at the polls because its role can be changed at any time, should another PopulexSlate fail in the polling place on Election Day.

From a voter's or poll worker's viewpoint, the PopulexSlate features the following:

- A smart-card slot to insert and read (or program) the smart-card voter election keys;
- A printer slot to insert a blank ballot, with a matching slot where a printed ballot is ejected from the PopulexSlate device;
- A touch-screen interface for the voter or poll worker to interact with the PopulexSlate device. This touch screen will only accept user input using a special stylus attached to the PopulexSlate. It will not react to human touch, or the touch of other objects such as a pen;
- A standard numeric keypad that can be used for straight numeric input, such as the PopulexSlate password, or for ballot navigation in audio-ballot mode; and
- A hand-held barcode scanner to read the barcodes on the Populex ballots.

The internal components and software of the PopulexSlate are all COTS products. The vendor argues this allows the PopulexSlate to be priced at the lowest possible level.

Ballot and report printing are performed by the Lexmark Z605 (or Z615) inkjet printer housed inside the PopulexSlate.

The core, and the "brains," of the PopulexSlate is a Compaq TC1100 tablet PC, which serves as the central processing unit of the PopulexSlate, as well as the touch-screen interface with which the users interact. (It should be noted that the Wyle Laboratories, Inc. report of February 1, 2006, indicates that the PopulexSlate includes either the Compaq TC1000 or the TC1100. The vendor represents the TC1000 is no longer available and only TC1100 units will actually be used in production.) The TC1100 is a fully functioning personal computer, featuring a removable 20 Mb hard drive, as well as USB, infrared and Ethernet ports. *The TC1100 includes a built-in wireless network interface, although the vendor states that the units are manufactured and shipped with this interface disabled.* The PC is attached to the PopulexSlate chassis and held in position by Velcro.

The PopulexSlate's TC1100 runs on a version of the Microsoft Windows XP Tablet PC edition operating system. The PopulexSlate's application software, Polling Place Functions (PPF), runs as a shell if the user logs onto the operating system using the standard operator password. This shell is reasonably restrictive and appears to confine the user to the PPF application, *unless the user shuts down and restarts the*

TC1100. The alternate administrative password provides full access to the TC1100 PC, including:

- Full read/write access to the hard drive, with sufficient permissions to install executable files;
- Full access to the Windows control access, including permission to modify & reset passwords; and
- Administrative access to enable or disable operating system services.

The PopulexSlate's housing or cover is a heavy-duty molded plastic. There is no built-in physical lock to secure the housing. Instead, the housing is secured by a small metal tab on the chassis that extends through a slot in the cover. This metal tab has a small hole through which a small lock (such as a luggage lock) or a tamper-evident seal can be placed. *While this mechanism appears insufficient and fairly easy to circumnavigate to access the internal components of the PopulexSlate, it may be sufficient to make such unauthorized access detectable.*

Further, the design of most modern voting equipment provides differentiated levels of physical access. For instance, memory ports or poll worker controls can be accessed through separate locked access doors, without providing full physical access to the rest of the hardware components. With the Populex PopulexSlate, no such differentiation on physical access is provided – it is all or nothing. *The cover must be fully opened for maintenance tasks such as installing the election definition and programming, replacing the printer ink cartridge, or resetting the printer paper guides, exposing every internal component of the device.*

2.2. Populex EMS Election Management System, version 3.05

The Populex EMS is a software application and database that is used to define and configure an election, to program the PopulexSlate devices, and to import vote results from the PopulexSlates, and then to compile and report those vote results.

The EMS application and database was developed in MS Access and MS Visual Basic for Applications.

The application is fairly limited in scope, but does support persistent jurisdiction district definitions from election to election and multiple election definitions. The reporting capabilities are extremely limited and restricted to the application's predefined reports, although data can be exported in several formats for manual manipulation by a user..

2.3. Populex Paper Ballot

The Populex system features a printed paper ballot that is "voter verifiable". The ballots are 5" x 10" and feature a header that can be tinted and watermarked in accordance with State law.

A voter on the Populex system is provided a blank ballot, which does not contain any contest information or timing marks. When the voter is ready to finalize his or her ballot, the ballot is inserted into the PopulexSlate for printing.

The finalized, printed ballot contains a two-dimensional barcode in standard PDF-417 format. This barcode contains:

- Basic information to identify the ballot style (precinct and party);
- The voter's choices for each contest as "punch positions" (candidate/ballot measure numbers); and
- An encrypted security key for ballot validation, to protect against counterfeited ballots.

The ballot style and vote choices are not encrypted within the barcode and can be verified independently by any PDF-417-enabled barcode reader.

The voter's choices are also printed in human-readable clear text on the ballot, in the form of candidate/ballot measure numbers, known as "punch positions". These numbers are readily verifiable, assuming the voter has access to a table that can translate from the candidate's or ballot measure's punch position number to the actual name of the candidate/ballot measure decision (yes/no).

For write-in votes, the barcode contains only the "punch code" for that contest's write-in position. The clear text portion of the ballot will contain both the write-in punch position *and* the write-in name in clear text. Electronic ballot verification and tabulation only records that a write-in vote was cast, not the actual name of the write-in candidate.

3. System Usage

3.1. Pre-Election Programming and Set-up

The Populex EMS is used to define a specific election, its contests and candidates and then to program the PopulexSlate devices to conduct that election. Districts are first defined within the system, and then contests assigned to those districts. Precincts are assigned voter codes, which are the key to the distinct combination of districts and contests belonging to that precinct. These definitions are persistent and can be used as a template to define new elections.

The Populex EMS supports multiple elections as long as they are not being held on the same date. Unfortunately, while configuring and editing an election, *election changes, including vote results, are not automatically saved.* Before switching between elections, the user must remember to "archive" the current election first, or all changes after the last "archive" will be irrevocably lost. While the application presents a pop-up reminder and warning before the switch is made, the warning defaults to the "Continue" button, rather than the "Cancel" button, *making it easy for a tired or harried election official to accidentally lose hours of work.*

The Populex EMS does not support ballot rotation. (In fact, *the current Federal NASED Qualification of the system specifically restricts it to jurisdictions without ballot rotation.*) Each candidate within a contest is assigned a "punch number". Candidates are listed within a contest in numerical order by this punch number. This means, to achieve ballot rotation for a contest, multiple logical contests must be

defined within the system, each containing candidates with identical names but different candidate/punch numbers. Logically, the election definition sees these as separate candidates who coincidentally have the same name. Because these are logically separate contests, there is currently no way to combine and report vote results from the separate versions of a contest within the system – this must be done manually by the jurisdiction.

This limitation of the EMS severely increases the risk of introducing errors in the election definition and, therefore, increases the burden of proof reading to prevent those errors. For example, the same candidate must be entered into the system multiple times (once for each rotation), each time introducing the risk of spelling or other definition errors, and each time creating another definition that must be carefully proofed. Finally, jurisdictions must exercise care when contests are assigned to a voter code (and thereby, precincts) to be sure that the correct version of the contest, with the correct rotation, is assigned to the voter code.

Synthesized speech audio ballot is configured through the Populex EMS. This Populex system only supports English and Spanish. General audio ballot navigation instructions are recorded by the vendor as .wav files and are included as part of the application. This means that these instructions are not readily changeable by the jurisdiction. Actual audio contest data (contest names, candidate names and ballot measures) are produced using synthetic speech. There is no capability to record or play back this information as analog .wav files. For candidate names, pronunciation can be fine-tuned using the phonetic pronunciation tool. No such phonetic pronunciation tool exists for the ballot measures. *This would make it extremely difficult or impossible to correct mispronunciation of words in the ballot measures' synthesized audio feed.* Finally, it should be noted that there is no published standard or guideline for using this tool. It is a matter of trial and error for the user to generate the correct pronunciation using the tool.

The entire election definition is exported to each and every PopulexSlate. Once the election definition is completed, a subset of that data is saved to a standard USB memory stick as an MS Access database. The PopulexSlate is then programmed for the election by starting the PopulexSlate's PPF application with the memory stick inserted into the PopulexSlate's tablet PC. As the application loads, the user is prompted for an election's digital signature (numeric hash). If the tablet's database does not already include an election definition for that data, the memory stick is checked for such a definition and, if found, the definition is automatically loaded onto the PopulexSlate.

This means that each PopulexSlate contains all ballot styles for an election. The vendor notes that this means that jurisdictions do not need to carefully track which PopulexSlates are programmed for which jurisdiction. It must also be noted that, *once deployed, there is no capability to lock down that PopulexSlate to a particular precinct or set of precincts and their appropriate ballot styles.* As discussed below, this increases the risk of poll workers issuing the incorrect ballot to a voter.

3.2. Opening the Polls

Poll workers logging on to set up the PopulexSlate and open the polls must have the PopulexSlate's Windows operating system password, the PPF application password, and the Judge's Election Key. The application password is necessarily limited to a numeric password that can be input using the PopulexSlate's numeric keypad. The Judge's Election Key is a smart card that simply contains the election date.

Upon successful logon, the user must then progress through each of the following steps:

Calibration of touch-screen is forced. This process is simple and straightforward, and ensures the PopulexSlate will accurately record user interactions.

User is required to confirm or reset the system clock. The user is presented with a screen that displays the system clock for the PopulexSlate and asks the user to confirm that the time is accurate or to correct the time. Unfortunately, *this makes it easy for the poll worker to accidentally or intentionally reset the system clock to the wrong date or time.* This would mean that all activities in the PopulexSlate's logs would receive the wrong time stamp. (e.g., could indicate such things as the polls were opened at 3:00 p.m. on Thursday.) (It should be noted that the vendor reports the system log would indicate the event of the system clock change.)

User assigns the station type for the particular PopulexSlate device. The user must tell the slate whether it is to function as a Judge's Check-In Station, a Voting Station, a Voter's Personal Verification Station, or as a Ballot Counting Station.

Additionally, one or more of the following actions may be required, depending on the role assigned to the PopulexSlate:

Bar code scanner is tested with a known test ballot (Verification Station and Ballot Counting Station configurations only). This step requires a specially printed test ballot to be included in the poll workers' supply kit. Alternatively, an alternate station can be used to print a test ballot.

A test ballot is printed and scanned to verify that the printer is working correctly (Voting station configuration).

A zero-report may be printed to verify no votes have been tabulated on the PopulexSlate device (Ballot Counting Station). It should be noted that this report is not automatically forced prior to tabulation.

3.3. Polling Place Operation

Once a new voter has been verified as eligible to vote, a poll worker programs an Election Key (smart card) for the voter on a Judge's Check-In Station. This key contains the ballot style and party information for that voter, as well as the accessibility support required for the voter.

The voter is given the Election Key and a blank ballot. The voter then inserts the Election Key into a Voting Station to activate the station and vote his or her ballot. When the voter is done, the ballot is printed with the voter's vote choices. The PopulexSlate's interface prevents over-voting and provides warning for under-voting. The PopulexSlate provides an audio ballot mode for accessibility. Other modality interfaces are supported, but these were not observed or tested.

The voter may take the ballot to a verification station and scan the bar code on the ballot to have the ballot's vote choices displayed or read back to the voter. Alternatively, the voter may verify the ballot by looking up the plain text "punch codes" on the ballot against a print-out that translates those punch codes to actual candidate names and ballot measure choices.

Once the voter is satisfied that the ballot accurately reflect his or her vote choices, the voter can go to a Ballot Counting Station and scan the ballot before dropping it into the ballot box. Alternatively, the ballot can simply be deposited into a ballot box for later tabulation.

Some of the more significant issues noted with this system include:

All ballot styles are available on the Judge's Check-In Station for creating Election Keys, thereby increasing risk of incorrect ballot style assignment to a voter. As noted previously, the PopulexSlate is always programmed with the entire election definition and all ballot styles. Unlike most voting systems, the PopulexSlate cannot be locked down to a specific set of ballot styles for the assigned precinct. Because the poll worker must identify the precinct/ballot style for each voter Election Key, there is a significant risk of choosing the wrong ballot style.

The PopulexSlate Voting Station is designed to display the jurisdiction's election official's name and signature at start-up. In California, this would likely be a violation of State laws prohibiting electioneering at the polls for elections in which the election official is running for office. The vendor must provide a workaround to suppress this feature for California use of the system. (While the vendor has told us this can be done, that work-around has not been tested.)

Manual, visual verification of the ballot is complex. Some voters may not trust the PopulexSlate verification system, since it is essentially the same system that recorded their vote choices and printed the ballot. The clear text printed portion of the ballot only lists "punch numbers". A separate printed reference is necessary to translate these numbers into contests, candidates and ballot measure choices. While the Populex EMS application does feature a "punch number report" for cross-references, the vendor acknowledges that the report is not in a voter-friendly format.. It is incumbent on the jurisdiction to reformat and print this data in a manner that is usable by the voter. Although the vendor suggests that this cross-reference information should be posted in the voting booth, it is questionable whether there is enough room to accommodate all the various lists

that would be required, particularly in a primary election with multiple political parties and in polling places that integrate multiple precincts.

Touch screen cannot be blanked for blind voters to protect their votes from being observed. Unlike many voting systems, the PopulexSlate does not provide the blind voter with the option to blank the display screen. Consequently, it is possible for someone to observe the blind voter's ballot choices unbeknownst to the voter.

Nothing prevents a voter or poll worker from double-tabulating a ballot. As originally designed, each Populex ballot in this voting system contained a unique ballot identification number to prevent a ballot from being scanned and counted multiple times. California has determined that the unique ballot identification number is prohibited by State law, and the vendor has subsequently removed that number from the ballot for the California version of the system. Unfortunately, that puts this voting system at risk for accidental or intentional mis-tabulation of the vote results.

Most voting systems prevent double scanning of ballots (or at least make it extremely difficult to do so), by physically capturing custody of the ballot as it is scanned. In the system configuration where the voters scan their ballots throughout Election Day, the voter must hold the ballot under a bar code scanner and then manually drop the ballot into a ballot box. Nothing prevents the voter (or a poll worker) from scanning a ballot more than once. While basic ballot accounting can inhibit this, such accounting would be fairly simple to circumnavigate. For example, a poll worker could double-scan a ballot that contains the punch code of a particular candidate and then, later, drop an adverse ballot into the ballot box without scanning to keep the ballots cast counts balanced. For this reason, tabulation must not be done by voters and poll workers throughout the day. ***At an absolute minimum, if this system is approved, the risk of fraud in tabulation must be mitigated by strict rules and procedures for careful tabulation after the close of the polls that include careful observation of the tabulation by multiple parties, as well as careful ballot accounting.***

The Populex system provides no electronic support for provisional ballots. If such ballots are cast on the PopulexSlate, they must be physically segregated and processed in the same traditional manner as provisional ballots in other paper ballot systems. Alternatively, the jurisdiction may want to use their existing absentee ballot system for provisional voting.

3.4. Closing the Polls and Canvassing the Votes

As noted in the previous discussion, tabulation of this system must be done at the close of the polls. Careful procedures should be in place to ensure the accurate tabulation of the ballots, and prevent accidental or intentional tabulation errors. Once tabulation is completed, the vote results are printed out on bar-coded (PDF-417) reports. These reports should be returned to the central tabulation center, together

with the ballots, where the barcodes on the reports can be scanned to aggregate and report the vote results for the canvass.

The Populex EMS is extremely limited in reporting capabilities, and is limited to the strict set of predefined reports in the system. The canvass reports are limited to county-wide aggregates and individual precinct results. There is no capability for ad-hoc report generation. This raises at least two significant issues:

Ballot rotation requires manual aggregation of the precinct returns. As noted previously, the system does not support ballot rotation and contests with ballot rotation must be defined as separate contests with separate candidates that happen to have the same names. Logically, within the system these are separate, disconnected/unrelated candidates whose results cannot be combined. Consequently, *jurisdictions with rotations must manually aggregate the vote totals from the various ballot styles to report the canvass.*

The system has no capability to aggregate and report vote results by sub-districts within the jurisdiction for specific contests, as required by the Supplement to the Statement of Vote. Current election law requires that jurisdictions report aggregated vote results for specific contests, such as US President, Governor and statewide ballot measures, by the Congressional, Assembly, State Senate, Board of Equalization, Supervisorial, and municipal districts within that jurisdiction. Again, the system has no capability to combine rotational contests and report results in this manner. *Consequently, jurisdictions using this system would be required to manually aggregate and calculate these totals, with a significantly increased risk of error.*

It must be noted that at the time of the system review, the vendor advised us that there was an existing Populex utility that might resolve these issues. That utility was not demonstrated or tested, and it has not yet been submitted to the ITA for qualification.

4. Security Concerns

While the vendor has attempted to address security of the voting system in many ways, such as the use of digital signatures in transferring the election definition from the Populex EMS to the PopulexSlates, the State's technical consultants and OVSTA staff had several security concerns with this system. The most significant of these are detailed in this section.

4.1. Verification of Trusted Software and Firmware

The vendor's original business model called for their strategic partner, HP, to supply the PopulexSlate tablet PCs and the EMS servers with a pre-configured image of the application software. When the vendor was queried on how they verified that the software installed was an actual copy of the qualified version, the vendor informed us that they just trusted this to happen.

We subsequently advised the vendor that this was not acceptable, and the vendor is in the process of redesigning the manufacturing and installation process. This had not

been finalized at the time of our review. At a minimum, the vendor must provide a clear means of independent version verification for system examiners and customers. Version self-identification, such as a help window displaying the software version, does not constitute such verification.

4.2. Microsoft Access as Development Platform

Security concerns have traditionally been raised over election applications developed in Microsoft Access, due to their inherent vulnerability of Access's Jet database engine to manipulation through native visual basic/DAO/ODBC connectivity from other Microsoft applications such as Excel. At a minimum, use and security procedures for this system must specify that no Microsoft Office or other Visual Basic-enabled applications may be installed on the EMS server or PopulexSlate tablet PCs.

4.3. Physical Security of System

As noted in Section 2.1 above, physical access to the PopulexSlate is not adequately prevented, although such access may be made detectable through the proper use of serialized tamper-evident seals. Further, physical access to components of the system is not differentiated and segregated to appropriate levels through the use of locked access panels as in other voting systems. Removal of the PopulexSlate cover and full physical access to the system is required to perform simple, routine tasks such as:

- Powering the PopulexSlate on and off
- Installing the election definition,
- Changing the printer cartridge, and
- Resetting the paper guides on the print

This is of particular concern because the heart of the PopulexSlate device is a full-fledged tablet PC. The tablet PC is held in position on the chassis with Velcro, making it a simple matter to remove the tablet from the chassis. Once removed, it would be just as simple to remove or swap the hard drive. It would also be a simple matter to access the ports to insert devices such as wireless network interfaces in the available PCMCIA slot or the USB port.

4.4. User Accounts and Permissions

Best practices generally dictate that security roles and permissions be defined such that a user has sufficient permissions to perform the required duties in a system, but no unnecessary permissions to perform other authorized functions . This Populex system, as presented, does not follow this practice.

For instance, the Populex EMS application has two types of user accounts/permissions: system User and Admin. The system user has full permissions within the application, except permission to create and manage other user accounts. This includes permission to create, configure and delete election definitions, export PopulexSlate programming, tabulate vote results, report vote results, and maintain

archived election databases. The Admin account has identical permissions to the general user accounts, plus permission to manage user accounts, including permission to: create new user accounts, reset passwords for those accounts, and assign Admin privileges to any user account.

In similar systems, one would expect to see separate account roles with suitably restricted permissions such as: election definition and maintenance; vote tabulation; election reporting, and system back-up. Because the security definitions are hard-wired into the EMS database, these are not easily changed without extensive modification of the application.

Similarly, the Windows logon for the PopulexSlate has two predefined accounts: Election Judge and Populex. The Election Judge account loads the Populex shell application which severely limits user access to the tablet PC's operating system. By necessity, the password for this account is limited to simple numeric characters that can be input from the numeric keypad. Unfortunately, the Populex account provides full administrative access to the PopulexSlate's hard drive and operating system, including the ability to: access control panel applets: enable and disable operating system services; add, delete and change passwords for user accounts; add new hardware (such as a wireless network card); and add or delete files from the hard drive, including installation of executable files. Even worse, the administrative password to the PopulexSlate is necessary to calibrate the printer after installation of a new ink cartridge – a process recommended before every election.

Finally, the PopulexSlates are configured to use the Windows XP "friendly logon" where each user account is presented as an icon to be clicked. Once clicked, the user is prompted for the password associated with this account. This is much less secure than the more traditional Windows logon, which requires the user to supply both the account's user ID *and* the password.

5. Other Concerns

Other concerns that were identified during the review:

Federal qualification issues. The current federal Populex system qualification specifically excludes jurisdictions that require ballot rotation. Under Section 19251 of the California Elections Code, the PopulexSlate almost certainly meets the definition of a DRE device and therefore is required, under Section 19250 of that code, to have received federal qualification before that system can be approved for use in California.

Security log and hard drive space. The PopulexSlate features a 20 Mb hard drive for data storage. The vendor advised us that if that hard drive fills and the security log (which records all events on that PopulexSlate) can no longer write to that log file, the PopulexSlate will "crash" There is no mechanism in the PopulexSlate to purge that security log. Instead, the entire hard drive must be re-imaged. Therefore, the vendor must specify in the system use procedures specific procedures to check hard drive storage space prior to each election to ensure that no PopulexSlates could fail midway through an election.

6. Conclusion

The Populex voting system, as presented for our review, is clearly not ready for approval for use in California. The system has major flaws that must be addressed and corrected before it can be approved. Chief among these deficiencies are:

- **Federal qualification –** the exact system for which California approval is sought has not received Federal qualification. Further the only versions of the system that have been federally qualified have been qualified with a condition restricting that use to jurisdictions that do not have ballot rotation.
- **System verification –** There is no mechanism for the vendor, the jurisdiction or third-party observers to verify software versions of the applications installed.
- **Ballot rotation** – the system cannot see a contest in separate districts with different candidate rotations as the same contest for either ballot definition or tabulation of vote results. Consequently, individual ballot styles must be manually combined to calculate and report results in the semi-official and official canvasses.
- **Supplement to the Statement of Vote reporting** – the system cannot provide vote results aggregated by sub-districts within a jurisdiction. This must be performed manually, adding the tallies from individual precincts.
- **Double-tabulation risks –** With the removal of the unique ballot ID required for California, the very nature of this system makes it vulnerable to accidental or intentional mis-tabulation of the ballots. It is questionable whether even the strictest of procedures can effectively eliminate this risk.
- **PopulexSlate system clock access** – Every start-up of the PopulexSlate provides the user access to reset the system clock, risking compromise of the system log.

Further, there are serious security flaws in the system design and implementation. These flaws should either be corrected or addressed in clear, comprehensive procedures for the system. Chief among the security concerns are:

- **Physical access to the PopulexSlate components** – The PopulexSlate cover must be opened, providing full physical access to the tablet PC and other components, to power the PopulexSlate on and off, or to perform routine maintenance tasks.
- **User account permissions not appropriately restricted** – The security roles defined for the EMS provide full administrative access to the entire application, except user account maintenance, to any user with a password. Similarly, any user with the Admin password has virtually unrestricted access to the tablet PC's operating system.

Finally, there were a host of less critical issues that affect the usability of the system in California. Some of these are the result of the system design, while others should be corrected in the short-term with use procedures, but should be addressed with modifications to the system in the long run.

- English & Spanish are the only languages supported;

- Ballot measure pronunciation cannot be readily corrected with the synthesized speech of the audio ballot;
- The PopulexSlate cannot be locked down to the appropriate precincts and ballot styles for the location to which it is deployed;
- The PopulexSlate does not force a zero-report before beginning ballot tabulation;
- Risk of data loss when switching between different elections in the EMS; and
- The PopulexSlate touch-screen cannot be blanked for blind voters using the audio ballot mode to protect their privacy.

While many of the issues identified with this voting system might be addressable through restrictive use procedures, this is not the preferred strategy. Human beings make mistakes, and sometimes procedures are not followed precisely. It is preferable, therefore, to address system issues through modifications to the system wherever possible.

In the case of the Populex system we reviewed, the number of issues identified with the system raises serious concerns about the viability of this system for use in California. While some of the shortcomings can be mitigated effectively with procedures, the sheer number of issues identified suggests a system that is immature and not appropriate for use in California by any but the smallest of jurisdictions, if at all, given the complexity of California elections and the elections environment.