Voting System Examination
Unilect Corporation

Prepared for the
Secretary of State of Texas

James Sneeringer, Ph.D.
Designee of the Attorney General

This report comprises the findings of the Attorney General's designee from an examination of the equipment listed, pursuant to Title 9, Chapter 122 of the Texas Election Code, section 122.036(b).

Examination Date	August 18, 2005
Report Date	September 11, 2005

Components Examined

Purpose	Component	Version	NASED #
Voting	Patriot Precinct Control Unit (PCU)	2.56 or 2.56f*	Not yet approved
Voting	Patriot Color Voting Unit (CVU)	2.54	Not yet approved
Voting	Patriot CurbSide Model	2.54	Not yet approved
Voting	Patriot Freedom Unit (Keyboard for disabled users)	1.0	Not yet approved
Scanning	Absentee Card Reader – Model 20	No firmware	Not yet approved
Election Setup & Tabulation	IntELLect Voting Software	2.61	Not yet approved
InfoPackerER	Memory Pack	1.0	Not yet approved

* See below for explanation.

Voting

Election Setup	Election setup is stored on the InfoPack, which plugs into the Precinct Control Unit (PCU)
Zero-total report	Yes.
Authorization to vote / Ballot selection	Poll worker authorizes voting at the Precinct Control Unit and tells the voter what booth to use, because all the stations are connected to the Precinct Control Unit.
View / Vote	LCD display / touch screen
Vote Storage	Ballot images are stored in the Precinct Control Unit, in two redundant static memories, powered by lithium batteries. There are four copies of the totals, in four redundant static memories, two in the InfoPack and two in the PCU.

Precinct Consolidation	Not necessary, since all votes are recorded in the Precinct Control Unit.
Transfer Results	Carry the InfoPacks or transmit by modem to election central.
Print precinct results	Yes, on the dot-matrix printer integrated into the Precinct Control Unit
Straight party / crossover	Yes. Crossover votes are retained when the voter changes the straight-party vote.
Challenged Ballots	Yes. The poll worker indicates at the PCU that it is a challenged ballot, and the display in the PCU gives the number of the challenged ballot.
Protective Counter	Yes, in the Precinct Control Unit, not in the voting stations.
ADA	Yes. Verified by the Secretary of State.

Election Setup / Tabulation

Results Storage	Flat file in proprietary format on the hard drive.
OS access	Not during tabulation.
Real-Time Audit Log	Yes. However, see below for a problem.
Transaction Processing	Precinct results are stored in a flat file, and changes to that flat file always affect only one record at a time, so any changes are always made in a single disk write. Totals are recalculated every time they are needed.

Issues from Previous Examinations

Note: *The vendor only listed the first item below on Form 100, Schedule A. The remaining items are the examiner's observations.*

1. A protective counter was added to the PCU.
   Result: This aspect of the system now complies with Texas law.
   Note: My records show that this was fixed before the last examination, but the UniLect listed it on Form 100, Schedule A,
2. The real-time audit log printer now works properly. It will not allow even a single event to escape logging, and during tabulation it properly logs any removal of the printer from the system. This is good, because removal of the printer could mean installation of a different printer in an attempt to conceal part of the real-time audit log. Also, the log now records each time someone manually updates the vote totals.
   Result: This aspect of the Patriot system now complies with Texas law.
3. The Patriot system no longer requires powering down when there is a problem with the real-time audit log. Instead it only goes back to the sign-in screen. (I believe it restarts the operating system.)
   Result: While this is an improvement, it is still a nuisance and demonstrates poor software engineering. However, while it annoys users, it is a minor annoyance that is unlikely to affect the integrity of the vote totals or the tally process.
4. The Patriot system no longer allows the votes from the same InfoPack to be counted twice.
   Result: This aspect of the system is now satisfactory.

5. UniLect's procedures now tell customers that the batteries that preserve the votes should be changed every eleven or twelve years (*Patriot Voting System User's Manual*, page 93-94).
   Result: This is an improvement, but still not satisfactory. See below under "Concerns."
6. The "Accumulate Results" button has now been re-labeled with a "*". This is an improvement, because it is used for things other than accumulating results, which made the instructions confusing in the old version. However, the change was made on the unit we examined by taping a "*" on the button; since the tape will quickly wear off, this is not very satisfactory. Also, the User's Manual still refers to "Accumulate Results" in many places, although I did find one note (on page 129 of the *User's Guide*, near the top) explaining that it has been changed to "*."
   Result: This is still not satisfactory, and illustrates the lack of professionalism that pervades the Patriot system.
7. Log files are now encrypted to prevent tampering.
   Result: This is an improvement.
8. UniLect did bring all the necessary equipment to the exam this time.
   Result: We were able to test every aspect of the Patriot system.

Other Changes

9. UniLect has improved the backup procedure. The system now makes automatic backups of vote totals by making a copy of the election data onto another hard drive.
10. UniLect now runs their software on Windows 2000 instead of Windows 98. Windows 2000 will be supported by Microsoft for a longer period of time than Windows 98.

Concerns

11. A record of each ballot is stored in the PCU in static memories powered by two independent sets of lithium batteries. Battery power must be supplied continuously for the votes to be preserved.

    Although there are two batteries in each InfoPack and two in each PCU, the vendor admits that there is no warning until the second battery fails, at which time any votes are lost. There is still redundancy, because the data is stored in both the InfoPack and the PCU. However, since the batteries are very likely the same age, it is conceivable that both would fail on the same day, thereby losing all record of the votes cast.

    UniLect requires that customers "arrange with UniLect for replacement of these batteries between eleven and twelve years from the date of purchase of the equipment, and every eleven to twelve years thereafter." [User's Manual, Section 11.2.2, page 94] This is an improvement since the last examination.

    UniLect also gives a procedure (in that same section) for testing the batteries by checking the voltage. However I can find no recommendation or requirement that the batteries be tested. Furthermore, when I suggested that checking the voltage might not be a sufficient test, they replied that the test should be performed "under load." However, I cannot find in the manual any mention of the need to test under load, or any procedure for testing under load. It appears that customers will have no way of knowing about the need to test under load.

Finally, UniLect says that they have a circuit that always uses the weaker battery in each pair of batteries, so that one battery will be preserved to keep the data alive. This is a good idea, if there is some notification when the first battery fails, but UniLect did not mention any such notification and I can find nothing about it in their manual. The negates the purpose of the design, since the customer will not know anything is wrong until the second battery fails, at which time that copy of the votes is already lost.

Also, when I asked UniLect how they tested the battery-switching circuit, they replied that they have not tested it, but are relying on the specifications from the manufacturer of the parts. This is unsatisfactory and exemplifies the general lack of forethought evidenced in the design of this system. Good engineering practice calls for extensive testing, especially for critical functions.

Finally, UniLect stated during the exam that you cannot use a voltmeter from the hardware store, but this fact is not documented in their manual that I can find. This is another important piece of information (since there are votes at risk) that has been glossed over by UniLect.

There are more secure ways to store votes, and this method (or any method that requires continuous power) entails unnecessary risk. In an age where reliable flash memory can be purchased at any computer or office store for as little as $20, there is no reason for UniLect to use memory that requires continuous power to preserve its contents. Furthermore the vendor has not demonstrated that they have procedures in place to ensure that battery failures will not result in lost votes.

Recommendation: Certification should be denied until such time that votes are stored on a reliable medium that does not require power. This technology is obsolete and should not be used.

12. The system is very difficult for precinct, central count, and warehouse workers to use. Many operations require knowledge of steps that are arcane and difficult to remember. For example:

(a) To cancel a ballot, you press the "16" button, followed by the button for the voting station. (I had trouble finding the documentation for this because it is in the Troubleshooting section, even though it is a normal Election Day procedure.)

(b) To reconnect a voting station, you press the button labeled "Accumulate Votes" or "*" followed by the "9" button.

(c) Errors are identified by numbers, which must be looked up in a manual.

(d) Adding a modem to the system requires editing a hexadecimal string.

(e) During the exam, a UniLect representative recited the steps to be followed after inserting an InfoPack. They were 13,14,15,*,13,14,15,*,14, hardly an understandable or memorable sequence. I believe this is done by back-office personnel, not precinct workers, but it still serves to illustrate the poor usability of the Patriot system.

This is not just a theoretical concern. Unilect admits in a letter dated, April 27, 2005, that they have lost vote records in Pennsylvania and North Carolina. In each case, they blame it on errors made by election officials, but in each case, the human errors should have been caught by the election system. In Pennsylvania, they blame a miscoded ballot and failure to follow test procedures, but the system should refuse to use a ballot if tests have been skipped. In North Carolina, they blame election officials for allowing too many ballots to be cast with a single control unit and for ignoring the warning messages, but their control unit could have prevented the damage if it had simply stopped accepting votes, rather than continuing to

allow people to vote when the votes were not being properly recorded. These examples reinforce and validate my point.

UniLect says that the problems that caused these incidents have now been fixed, but they still serve to illustrate the inadequate testing and neglect of usability engineering at UniLect. The anticipation of every possible problem and thorough testing of software is a critical part of software engineering. It is essential that problems be discovered in the laboratory, not in the precinct, where votes can be lost, as they have been in the history of the Patriot system.

This system does not even approach the state of the art for ease of use, especially for a system used by pollworkers, who are infrequent users, usually with minimal training. Note that these are just samples of problems found in a short time. There are probably many more.
Recommendation: In my professional opinion, confirmed by field experience with the Patriot System, this system does not meet the state requirements for efficiency and ease of use. It should not be certified until this is fixed and it is re-examined.

13. Absentee voters must consult a separate list of races, determine the number of the candidate they want to vote for, and mark that number on the ballot card. Many voters will find the use of candidate numbers to be difficult and error prone.
Recommendation: The method of absentee voting should be improved before the system is certified for that use.
14. The Patriot system uses a confusing version number scheme that should be changed. On Form 100, UniLect listed the version number of the PCU as 2.56, but the actual version number of the system we examined was 2.56f. The explanation was that the *f* indicates an internal version number, and it will be removed before the product is shipped. As an examiner, I find this very frustrating, because (a) it means that several different versions presented to us will have the same version number, making it difficult to track changes, (b) that it is difficult for us to determine if the version we examined is the version that was shipped, and (c) that it is difficult for us to determine if the version we examined is the same one that was approved by the ITA. Shortened version numbers are fine in marketing materials, but the version numbers submitted to the Secretary of State and the version numbers displayed by the software itself should always be different whenever the software has changed, and the version numbers should always increase over time, and never decrease. (An example of a decrease is going from 2.56f to 2.56.)
Recommendation: In the future, certification should be denied unless version numbers meet these criteria.

Summary

UniLect has been responsive and has fixed many of the problems raised in past exams. They deserve credit for listening and taking action to address some of the concerns of the examiners.

However, the problems are so pervasive that the Patriot system should not be certified until it has been re-engineered using up-to-date software usability techniques, performing system tests in accordance with established hardware and software engineering practice, and avoiding memory that requires continuous power to maintain the vote totals. UniLect needs to anticipate and protect against attacks, user errors, and other real-world situations that can jeopardize the voting process. I would suggest that they engage outside consultants in the re-engineering process, to help identify and protect against potential weaknesses that might be missed by a very small

development team. In this situation, there is strength in numbers. Having several different viewpoints is essential, because designing for security and data integrity requires an in-depth approach.

Certification of the Patriot system without this kind of systemic changes would expose Texas to a significant risk of lost votes or other incidents that might delay results, engender confusion, cause challenges, and undermine public confidence in electronic voting.

UniLect seems much more interested in squeezing through the examination than in producing a high quality, robust system that will protect the integrity of Texas elections. They seem to do the minimum they can get by with to address examiners comments. (In one instance, they literally used tape to fix a problem, and then failed to document the change adequately in their manual.) Furthermore, they do not seem very concerned about the votes that have been lost by their system, seeking to place the blame on election workers. I disagree with this approach and this philosophy. A computer system (and especially a critical system such as an election system) should do everything it can to prevent possible errors of all kinds, including user errors. Where this is not possible, the design should minimize the impact of mistakes. This is especially true for election systems, which are used infrequently and by people with minimal skills.

The large number of problems with the UniLect system puts examiners in an awkward position. A three-hour examination of an election system is like a financial audit, which cannot guarantee the correctness of an organization's books, but only checks a limited number of transactions. When an audit finds a high rate of errors, the books are not considered reliable even after the known errors have been fixed, because the transactions that were not examined probably have a similarly high rate of errors. This principle also applies to the Patriot system. Because a large number of problems were found in a short period of time, we can conclude that UniLect's engineering process is not producing reliable results. UniLect should revise its processes, possibly by seeking ISO 9000 certification or by using consultants. The Secretary of State should ensure that future UniLect examinations are sufficiently rigorous to protect Texas voters, especially if UniLect does not improve its engineering process.

If any prior UniLect systems are based on the same software or memory, they should be decertified to protect the integrity of Texas elections. The case for decertification of older systems is even stronger than the case against certification of the system examined, because they presumably have the known problems that have caused the loss of votes in other states.