



Fairness. Accuracy. Democracy.™

POPULEX CORPORATION
420B AIRPORT ROAD
ELGIN, IL 60123
TEL 877.POPULEX (767.8539)
FAX: 562-684-3600
www.populex.com

April 17, 2008

Ms. Dianne Felts
Director of Voting Systems and Standards (VOSS)
1020 S. Spring St
Springfield, IL 62704-2924

Dear Ms. Felts:

I received your e-mail with the attachment "Populex Findings April 2008" on April 16.

Populex did not have a chance to review the report prior its being sent. As such and unfortunately, we were not in a position to either correct or comment on sections of the report that we believe are either inaccurate or misleading.

We believe that the Populex system is the **only** system in Illinois that meets specific federal accessibility standards.

Not having our comments on accessibility and security as part of the report may raise unnecessary concerns among citizens who want secure and accessible elections. We believe the security issues are unfounded and we present an item-by-item rebuttal to the points in your report in the attached appendix.

We request that our comments be made part of your report so that confidence in the electoral system is not unnecessarily undermined. We also request that our comments be made part of your report to avoid the risk that less secure systems become *de facto* standards in Illinois.

The report focuses heavily on features related to accessibility for voters with disabilities. Accessibility improvements can be made in any voting system. Accessibility weaknesses that exist in other voting systems in use in Illinois certainly do not excuse us from making improvements in ours. However, the perceived weaknesses mentioned in your report are not based on any federal standard.

On the other hand, as voters in Illinois, we believe that systems made by others (those on which we vote) do not meet federal requirements. Populex, as far as we know, makes the only system that meets **all** of the federal accessibility requirements.

We provide an examples for your consideration:

Example: The 2002 Voting System Standards ("VSS") provides that an electronic display **shall** [emphasis added] allow the voter to adjust the color and contrast of the display (See 2002 VSS 2.2.7.2 e(1) and VSS 2.2.7.2 e(2))

Populex staff and other parties voted on a variety of systems in use in Illinois in the 2008 Primary Election. As far as we know, none of those systems met this federal requirement for adjusting the color and contrast of the screen.

The machines on which several of us voted as recently as last February did not meet this federal requirement. We have no reason to believe that such accessibility requirements are optional. They are, however, implemented in the Populex system.

This example is not the only cases in which the Populex system meets federal requirements and others appear not to.

We readily agree that one system's weakness is no excuse for another's shortcomings. However, each and every accessibility change you cite in your report is not based on any documented federal requirement, yet non-Populex machines in use in Illinois do not meet those requirements.

I hope you realize that this is not an apologia for improvements we certainly can make and have agreed to make. But, reciting the list without mentioning that the Populex system is probably the only system in use in Illinois that meets federal accessibility requirements raises the possibility that the reader may be misled. We note for the record that the Braille stickers mentioned in the report are available.

For fear of losing the forest for the trees, we do not comment on every point in your report but would be happy to do so if called upon.

While we rebut all security comments in your report in the appendix, we point out the following: **The Populex system produces an unambiguous, voter-verified paper ballot that is both counterfeit-resistant and multiple-counting resistant.** It is the only system that does that.


Comments on "Populex Findings"

April 2008

Page 3

We request that our rebuttal to the security concerns, attached as an appendix hereto, be made part of your report. The comments made in your report may unnecessarily lead to a diminution of confidence in Illinois's electoral systems in use in Sangamon County. We hope to avoid that; it is not called for.

Yours truly,

A handwritten signature in blue ink that reads "Sanford J. Morganstein". The signature is written in a cursive style. Below the signature, there is a faint, light blue watermark or stamp that is partially obscured and difficult to read, but it appears to contain the name "Sanford J. Morganstein" and some other text.

Sanford J. Morganstein
President

APPENDIX

RE: ILLINOIS STATE BOARD OF ELECTIONS POPULEX FINDINGS APRIL 2008

Page 24 of the referenced report recites seven “security concerns.” Because this is of the utmost importance in the design of the Populex system, indeed any voting system, Populex comments on each of these concerns. We regret that you did not give us the chance to comment to your staff on what they report as security issues. The factual recitation provided below should traverse those concerns. But, if not, reflection on how the Populex system changes the overall security paradigm should alleviate these concerns. Nonetheless, we address each concern.

- The HP Tablet PC comes with Ethernet and infrared ports.

State law prohibits **external** infrared ports. The infrared port in the Populex machine is **internal**. Furthermore, the infrared port is securely disabled. The Ethernet port is also securely disabled.

These are not mere semantic distinctions. We certainly agree that any active Ethernet or infrared port may be dangerous...especially in a DRE system (which the Populex system is not). We anticipate an argument that anything that is “disabled” can be “enabled.” Yes. However, anything that has a computer attached to it, including optical scan precinct tabulators, can have an infrared or Ethernet port added to it. From a security point of view, there is no meaningful difference between a port that that is disabled through more than one security mechanism (as is the Populex system), including physical locks, and any other machine that can have anything added to it on a simple plug-in basis.

Having a secure approach does not give us license to ignore the State’s Election Code: We do not; we comply to the letter of the requirement. However, for the record, we point out that the overall design of the Populex system renders all those security attacks moot because the Populex ballot has anti-counterfeit measures and further measures preventing a ballot from being counted more than one time.

Finally, please recall that **no Populex voting machine stores vote data** on it. The precinct tabulator does store vote data, but that data comes from inalterable, unambiguous paper ballots stored in a physically locked ballot box in the county clerk’s secure vault. Those unambiguous, counterfeit-resistant paper ballots may be used to verify and audit the tabulator’s results. Such audit or verification may be performed by “hand” or machine.

- The Technical Data Package offers no support for verifying software versions.

You may be aware that the question of verifying appropriate software versions is a problem that is under investigation by federal experts. But, more importantly, the Populex system renders such verification moot. The Populex ballot has anti-counterfeit provisions and a Populex ballot cannot be counted more than one time. Unlike other systems in use in Illinois, the Populex paper ballot is easily auditable without revealing the identity of the voter.

We do not believe the State Board ever communicated to us a concern about version verification before this report.

- Election Judges can set the time and date on a polling place machine “which could result in audit logs becoming meaningless.”

Had we had the chance to discuss this with you, we think you would see that such a statement is without merit and perhaps counterproductive. Simply put, the audit log is sequential¹, not time ordered. Furthermore, if a poll worker changes the time, an audit log entry is made. The logs are therefore secure and far from meaningless. On the other hand, if a clock could not be set by election judges (presumably one from each party) and if the clock drifts, as all computer clocks are wont to do, the audit log would have wrong time and date stamps. Federal requirements force time and date stamps in log entries. Not being able to auditably change a clock will ultimately result in inaccurate time stamps.

- When the computer is configured to serve as a precinct tabulator a zero report is not the result of an automated function.

The system is designed so that it cannot be set as a precinct tabulator *without* all counters being set to zero. Also, a permanent log entry is made when the counters are zeroed. The permanent log is available, as is an understanding of the operation of the system, should a zero report be required for any probative reason.

But, perhaps more important, the Populex system produces an inalterable, voter verified ballot that is counterfeit-resistant double counting resistant.

¹ This discussion pertains to the internal audit log, not the sequential paper roll used in certain DRE machines. Such sequential paper rolls, not used by Populex, pose a strong risk of violating the fundamental concept of a secret ballot. This is especially true in Illinois where poll workers are required to announce the identity of the voter when the voter presents himself or herself.

Any proof as to the accuracy of a precinct’s vote counts has the best record available: the voter’s inalterable, unambiguous statement of intent.

Finally, this requirement is covered in the 2002 VSS in § 2.3.5 e. The Populex system meets this requirement.

We add that the State Board started, or observed the starting of, these same machines probably close to scores of times during your testing. A zero report can be printed, the registers are always **displayed** to be zero, the audit log proves that the counters were zeroed and the unambiguous paper ballot is the ultimate proof of the correctness of the count.

We agree that complying with Board rules is not the open to a vendor’s choice. However, if the secure operation described above is impermissible from a regulatory point of view, such information was not communicated to us.

- The touch screen cannot be blanked for voters with visual impairments.

The touch screen can indeed be blanked by the simple method of placing a blank sheet of paper over it. In our work with focus groups we found that simple, intuitive approaches are better than unnecessarily complex, unintuitive, overly-technological approaches.

All functions operate properly with a sheet of paper over the screen which does “blank the screen.”

- The entire election [all ballot styles] is loaded into every computer.

Your report includes an article from the *State Journal Register* (April 8, 2006) describing how poll workers may have provided the wrong ballot to voters in a “split precinct.” In the reported incident, the poll workers selected the *proper precinct* but perhaps improper ballot style. The implication that precincts not in use be “locked out” would not have prevented this situation on our system or on any other system.

On the other hand, wrong ballots can be delivered via poll worker error. We have developed an approach, at the suggestion of Sangamon County officials, that would integrate “poll book” data with the voting machine. That approach solves almost all problems except those related to misidentifying

voters at the polling place or erroneous data entry. That suggestion has been implemented but not yet federally tested.

The improvement we describe is one of those incremental improvements that we agree would be an improvement, although as noted, it would still not solve all human error situations.

Having all ballot styles resident in all machines ensures that spare machines can be delivered promptly and furthermore reduces the chance of error of the wrong machine’s being delivered to the wrong precinct.

- “The administrative access to the system is inadequately password protected. Access...would not be difficult.”

We are not sure to what extent the person writing this comment is aware of the security of the Populex system. We review it here:

The computer BIOS is password protected. That password is not provided to pollworkers nor to county officials.

Access for pollworkers requires **two** different codes. The first code simply starts the voting application...no access to files or any other function is allowed. The password may be changed for each election. A second password **must** be changed for each election. Voting cannot begin until this second password is entered. The county can make the first password as complicated as they wish and can make the second password virtually as long as they wish.

Furthermore, voting cannot begin until an encrypted Digital Signature of the election file is entered and matched to prove that there has not been one single change to the data.

As to technical support personnel, they must also log on. The password for this access can be as long and complicated and “strong” as the county desires. Furthermore, if the county desires, that password can be changed as often as desired. Finally, the system can be set up to force the password to be changed at a desired frequency.


Respectfully, we believe that the combination of multiple passwords, encrypted Digital Signatures on the data file, encrypted check sums on the

Security Appendix to
Comments on "Populex Findings"
April 2008
Page 8

voter verified ballot that is counterfeit and double counting resistant makes the Populex system the most secure system available to the voters in America.

Again, we request that these comments be made part of your report lest unwarranted lack of confidence in the Sangamon County voting system result.

Respectfully submitted

A handwritten signature in blue ink that reads "Sanford J. Morganstein". The signature is written in a cursive style. The text is overlaid on a faint, light blue grid background.

Populex Corporation
Sanford J. Morganstein
April 17, 2008
President