STATE OF COLORADO
Department of State
1700 Broadway
Suite 250
Denver, CO 80290

Mike Coffman
Secretary of State

Holly Z. Lowder
Director of Elections

Voting Systems Testing Board
Major Deficiencies Report:
Election Systems & Software (ES&S)

February 15, 2008

Executive Summary

The enactment of House Bill 08-1155 provides the Secretary of State (Secretary) with increased authority over the testing process and allows for additional testing and communication with the vendors and counties by this office. The legislation allows for an order to decertify a voting system to be amended or rescinded if it is determined that the major deficiencies have been resolved or mitigated. As part of the decision to amend or rescind an order, HB1155 allows the Secretary to consider the "accuracy and security procedures, audits, processing functions, and other relevant procedures used by county clerks and recorders in accordance with the laws and rules governing the conduct of elections."

This report by the Testing Board addresses the major deficiencies identified by the Secretary in his order on December 17, 2007 (December 17 decision) decertifying the ES&S voting equipment. This report explains the additional information provided and additional testing that has occurred since the December 17 decision, and demonstrates that the decertified components are able to overcome the major deficiencies outlined in the December 17 decision.

Testing Board Findings

The ES&S Unity software, the M100 precinct scanner, the M650 central count optical scanner, and the iVotronic Direct Record Electronic (DRE) voting machine were all decertified by the Secretary for use in the State of Colorado. The major deficiencies identified were failure to detect election programming changes and errors; inability to determine if tabulation software worked correctly; inability to complete testing threshold of 10,000 ballots due to vendor programming errors; system vulnerable to security attack; and failure to provide auditable data to detect security violations.

Unity Software

The major deficiencies identified with the Unity software relate to the inability to "lock down" the database at a given point in time preventing changes to the system.

The Testing Board has created a process, as outlined in the **Conditions for Use** section of the "Election Systems & Software Voting Systems Project Overview – A.3.", to create a secured copy of the database to be the only "trusted" county database to be used. At specific times during the election process (Logic & Accuracy Testing, Memory Card Upload, Post Election Audit, and Canvass) the operators of the system will be required to use the secured copy of the database for election processing.

The process, when used in concert with county security procedures, will mitigate the system's failure to detect programming changes and errors and failure to provide auditable data necessary to detect security violations.

M100/M650 Optical Scanners

When the Testing Board began testing the optical scanners submitted for certification by ES&S, they discovered that the programming ES&S provided did not match the physical ballot definitions and therefore could not be used to test the scanners. Throughout the certification process the Testing Board communicated with ES&S to resolve the programming issue. ES&S provided at least five (5) sets of programming and three (3) sets of ballots, none of which were compatible with one another.

Because ES&S did not provide the correct programming and ballots, the Testing Board was unable to complete testing the scanners, including tabulation of 10,000 ballots as required by Secretary of State Election rules within the deadlines set forth for the testing process.

ES&S provided new programming and ballots that were compatible with one another. In late December 2007, the Testing Board began processing ballots with the new programming in an effort to complete testing. The tabulation of the 10,000 ballot threshold was successfully completed and verified as accurate.

iVotronic DRE

During the testing relating to the December 17 decision, the Testing Board discovered that by introducing a magnet into the area designed for the Personalized Electronic Ballots (PEB) the system could be powered down. This created the major deficiency of the system being vulnerable to a security attack.

The iVotronic DRE uses an infrared serial port to communicate with the PEB. The iVotronic hardware contains a magnetic reed switch which allows communication with the PEB. Along with the specific data necessary to identify the type of PEB being used, the PEB also contains a magnet which activates the appropriate reed switch inside the iVotronic.

The Testing Board found that the token activation system of the PEB process can be easily defeated. In response, the Testing Board has proposed a solution to mitigate each of these problems in the **Conditions for Use** section of the "Election Systems & Software Voting Systems Project Overview – A.3.".

The following list identifies the possible consequences of a PEB port attack:

Prematurely Cast or Cancel Ballot – When a magnet is inserted into the PEB slot, it can result in a ballot being cast prematurely or cancelled. In particular, the voter may be presented with a non-voting screen asking the voter to cancel or cast the ballot. The machine then resets for next voter without loss of votes or other data.

Reboot (power cycle) terminal – When a magnet is inserted into the PEB slot while pressing the vote button, the machine may power on/off the voting terminal between voters. A voter could, after successfully voting, power down the device. Upon power-up of device, which may also be accomplished by use of a magnet, instances of stack dump errors and other unrecoverable errors have occurred causing denial of service for the device. In the testing that was conducted by the Testing Board, there was not a finding that any votes or other data was lost or modified.

Unauthorized Recalibration – An unauthorized recalibration may be implemented by any supervisor programmed PEB; no password is required and the ability is specific to county or election specific data. Operators are capable of entering the calibration screen using a foreign Supervisor PEB, such as one purchased on the open market, from another jurisdiction, or a home made PEB emulator. The screen can be calibrated so that touching a desired point would be recorded by the machine as a touch at a different location. This could cause voter input for one candidate and selection recorded for a different candidate. During testing, the calibration was changed such that upon entering vote mode with the correct PEB, workers inadvertently closed polls. This type of attack causes denial of service.

In response to the security risk associated with the introduction of a magnet to the PEB port, the Testing Board recommends that a cover be placed on the DRE to mitigate the possibility of a malicious attack.

The Testing Board reviews and tests voting systems based on a standard of strict compliance. This means that any voting system that fails one test will not be recommended for certification. However, the Secretary's decision to certify or decertify a system is based upon the legal standard of substantial compliance pursuant to § 1-1-103, C.R.S. Factors to be considered under the substantial compliance standard include the extent of noncompliance with the Election Code and the purpose of the provision(s) violated and whether or not that purpose may be achieved despite the violation.

The information listed in the "Election Systems & Software Voting Systems Project Overview – A.3", the amended Project Overview binder, set forth the necessary conditions to be fulfilled in order for such equipment to be used should the Secretary certify the system for use in the State of Colorado.