

WASHINGTON



**Secretary of State
Elections Division**

**Report of the Secretary of State
on the examination of**

**Clear Ballot Group
ClearVote 2.3 Voting System**

April 2023

Table of Contents

OVERVIEW	3
Application	3
New Voting System.....	3
National Certification.....	3
Testing & Inspection	3
EXECUTIVE SUMMARY OF FINDINGS OF SECRETARY OF STATE STAFF	4
Voting System Accuracy.....	4
Results Reporting.....	4
Presidential Primary.....	4
System Limits	5
Ballot Scanning.....	5
Ballot Processing.....	5
System Security.....	6
Physical Security	6
Write-Ins	7
Accessible Voting	7
CONCLUSION.....	7

Overview

Application

In November 2022, Clear Ballot Group submitted an application for Washington State Certification of ClearVote 2.3. Clear Ballot Group applied to certify functionality several components of the ClearVote Voting System, specifically, ClearDesign, ClearAccess, and ClearCount. Copies of operating and maintenance manuals, training materials, technical and operational specifications were provided as part of the EAC's Technical Data Package.

New Voting System

This is a modification of a currently certified voting system (ClearVote 2.3) to the State of Washington. This system is a paper-based digital scan voting system with a commercial off the shelf (COTS) scanner.

National Certification

After the completion of testing by a certified Voting System Test Lab (VSTL) the Election Assistance Commission (EAC) certified ClearVote 2.3 on October 31, 2022. The hardware and software of the system that was approved by the EAC can be found in the EAC's Certificate of Conformance and Scope.

Testing & Inspection

Testing and evaluation of ClearVote 2.3 was conducted by Secretary of State staff at King County Elections in Renton, Washington, on March 28, 2023. Examining the system for the Office of the Secretary of State were Les Bowen, Voting Systems Lead, and Callin Silvernail, Election Integrity Lead.

Due to ClearVote 2.3 receiving National Certification from the EAC, a two-phase testing program was developed and approved by Secretary of State EIS Supervisor for state certification testing:

Delivery acceptance testing of the equipment and software to determine if the correct model and versions of the equipment and software are delivered and that the equipment, software, and system operate as documented by the vendor.

Election results testing to ensure that the equipment, software, and system perform each of the functions required by federal, state, and local law in order to administer an election from the beginning to the end.

Ballots were manually voted using the accessible voting unit, ClearAccess, and incorporated into the results to ensure proper tabulation.

Executive Summary of Findings of Secretary of State Staff

Voting System Accuracy

ClearVote 2.3 successfully and accurately tabulated all ballots including additional hand-marked and manually voted ballots from the accessible voting units. Results were manually audited and reviewed by a team of two.

Results Reporting

ClearVote 2.3 was able to produce the state required reports for election results by precinct and cumulative.

Presidential Primary

ClearVote 2.3 can perform all the functions necessary to comply with current state requirements for the Presidential Primary, which means it can detect cross-party voting in a Presidential Primary without manual intervention.

System Limits

This table, containing information from the testing lab certification test report, depicts the limits of the ClearVote 2.3 system, as stated by Clear Ballot Group.

Parameter	Limit
<i>Election Parameters</i>	
Precincts per election	3,200
Splits per election	3,200
District categories per election	100
Districts per single category	3,200
Districts per election	3,200
Contests per election	3,200
Choices per election	3,200
Choices per contest	300
Vote positions per side	420
Card styles per election	3,200
Contests per ballot style 60	60
Card styles per precinct 50	50
Parties per election 50	50
Counter groups per election 7	7
"Vote for" per contest 50	50
Languages per election 15	15
Cards per ballot (per language) 5	5
Write-ins per contest 50	50
<i>Reporting Name Parameters (Reports Only)</i>	
Election name (characters)	60
Jurisdiction name (characters)	60
Precinct name (characters)	60
Vote center name (characters)	60
Contest name (characters)	60
Candidate name (characters)	60
Party name (characters)	60
Write-in length (characters)	60
<i>System Parameters</i>	
Central-count scanners per network	10
Cards per precinct-voting device	10,000
Cards per central-count device	4,000,000

Ballot Scanning

ClearVote uses Fujitsu scanners capable of sustained scanning speeds of up to 130 ballots per minute using Scanner Model fi-6800 with a ballot measuring 8.5"x5", and as low as 20 ballots per minute using Scanner Model fi-7180 with a ballot measuring 8.5"x22". During testing of a ballot measuring 8.5"x14" we experienced a scanning speed between one and two ballots per second.

Ballot Processing

ClearCount is a central, high-speed, digital scan ballot tabulator coupled with ballot processing applications. The ClearCount software runs on unmodified COTS laptop or

desktop computers running the Windows operating system and supports specific models of scanners.

The ClearCount central-count system runs on an Ubuntu Linux operating system, with network connections to workstations running the Windows operating system. All the components are unmodified COTS that are connected via a wired, closed, and isolated network not connected to any other systems or the Internet.

System Security

ClearDesign and ClearCount require a server that stores the election data. That connection to the server is via a HTTPS connection through a VPN router capable of IP/MAC/Domain name filtering and other high security features. This is ideal for completely locking down the internal network in large counties.

All laptops and computers are hardened to restrict only approved (“whitelisted”) applications to be opened on each workstation along with securing and protecting other important areas of that workstation.

ClearAccess devices include a bezel that will cover and protect the exposed ports and only expose those required for accessibility and power. Those ports can be protected via a tamper evident seal when not in use.

All software and media have an easy-to-view hash checksum value that will ensure that the device’s software has not changed since its last install. Additional system and election event logs can be accessed to view any activity on that device. Furthermore, users can be given roles or credentials that limit their ability to perform any action on the system.

When Clear Ballot products start up, they check that the cryptographic module is operating in FIPS mode. If not, the product displays an error message and will not proceed.

Physical Security

An excerpt from Clear Ballot's security recommendations is:

When the components of any system are not in use, they must be stored in a locked area under the custody and control of the jurisdiction. Access to this area must be controlled by the jurisdiction so the system cannot be accessed by unauthorized individuals and any breaches in security can be recognized through the auditing functions of the system.

When in storage or in use, the ClearVote equipment must be kept within a controlled area. Only individuals authorized by the jurisdiction to handle and process ballots or to maintain the voting system can come into direct contact with the ballots or components of the system. Each jurisdiction must also follow all jurisdictional and state rules for the handling and processing of ballots. This means that at least one security method is employed to provide deterrence and physical security:

- Receptionists or guards with a gate or other barrier to the storage area.

- Security cameras.
- Electronic door-locking mechanisms such as ID cards or key fobs that record the identity of the device used to unlock the door.
- A locking computer rack or other cabinet to contain components of the ClearVote system.

The jurisdiction must record whenever any ClearVote equipment is brought out of storage. After setting up the system, examine the election log and system log to determine if any unauthorized access occurred while the system was not officially in use.

If there is a break in the custody and control of the jurisdiction, the jurisdiction must reverify the integrity of the system and, if necessary, reinstall it.

Write-Ins

ClearVote allows for entering write-in candidates after results have been enabled. Write-in candidates do not have to be on a qualified or declared list prior to ballot processing.

Accessible Voting

ClearAccess has an accessible voting unit that is touchscreen, can be used with the provided accessible switches or the voter's assistive technology, such as a sip-and-puff device. Once the voter has completed voting, their ballot is printed onto regular ballot paper. Depending on the county's procedures and in compliance with all other state elections law, the voter could then put their ballot into a return envelope and into a ballot drop box to be processed with all other ballots returned by mail or in drop boxes. The vote is not captured electronically, meaning this device is not a direct recording electronic (DRE) voting unit. Accordingly, this device does not need to be audited separately. The votes on ClearAccess will be a part of the post-election audit as the ballots can be mixed in with all other ballots.

Conclusion

After an evaluation of the system, staff believes the system and its components meet current Washington State requirements for Presidential Primary, Special, Primary, and General Elections.