



Clear Ballot

ClearVote 2.3

ClearCount Functionality Description

ClearCount Functionality Description

Clear Ballot Part Number: 100021-10020

Copyright © 2012–2023 Clear Ballot Group. All rights reserved.

This document contains proprietary and confidential information consisting of trade secrets of a technical and commercial nature. The recipient may not share, copy, or reproduce its contents without express written permission from Clear Ballot Group.

ClearAccess, ClearAudit, Clear Ballot, ClearCast, ClearCount, ClearDesign, ClearVote and the Clear Ballot eye logo are registered trademarks, and CountServer, CountStation, DesignServer, DesignStation, ScanStation, Visualization of Voter Intent, Visual Verification, and Vote Visualization are trademarks of Clear Ballot Group. Other product and company names mentioned herein are the property of their respective owners.

Document Type: Technical

Clear Ballot Group
2 Oliver Street, Suite 200
Boston, MA 02109
857-250-4961
clearballot.com

Document history

Date	Description	Version	Authors
01/10/2017	Initial submission to EAC	1.0	Joni G. McNutt
02/03/2017	Minor typographical and reference-related edits	1.0.1	Joni G. McNutt
04/28/2017	Minor updates based on feedback from the State of Colorado and Clear Ballot Quality Assurance	1.0.2	Joni G. McNutt
06/16/2017	Minor updates for vote-by-mail campaign	1.0.3	Joni G. McNutt
07/21/2017	Minor edits to fix typos, added information to the Accuracy and the Obtaining the ClearCount software sections	1.0.4	Joni G. McNutt
09/01/2017	Updated the Data retention section, minor edits	1.0.5	Joni G. McNutt
01/19/2018	Vote-by-Mail campaign 2	1.0.6	Joni G. McNutt
04/27/2018	Minor edits	1.0.7	Joni G. McNutt
06/01/2018	Updated cover	1.0.8	Joni G. McNutt
06/15/2018	Updated cover, minor edits	1.0.9	Joni G. McNutt
08/15/2018	Updated cover	1.0.10	Joni G. McNutt
02/12/2019	Minor edits to the Mark Analysis section	1.0.11	Joni G. McNutt
04/12/2019	Minor edits	1.0.12	Joni G. McNutt
11/22/2019	Minor edits	1.0.13	Joni G. McNutt
02/12/2020	Minor edits	1.0.14	Joni G. McNutt
12/15/2020	Added the following sections: <ul style="list-style-type: none"> “Consolidating from ScanStations” “Consolidating from ClearCast” Minor edits	1.0.15	George Petta
06/04/2021	Updated title-page verso. Changed all instances of ScanServer to CountServer and all instances of election administration station to CountStation.	1.0.16	Joe Srednicki

Date	Description	Version	Authors
10/21/2021	Minor edits	1.0.17	Eric Burz, Joe Srednicki
03/21/2023	Minor edits.	1.0.18	Kristina Arnold

Table of contents

Preface	10
Chapter 1. Overall system capabilities	12
1.1 Security	12
1.2 Accuracy	13
1.2.1 Recording contests, candidates, and issues exactly as defined	13
1.2.2 Recording votes accurately	15
1.2.3 Producing accurate, detailed reports	22
1.3 Error recovery	23
1.3.1 System and software errors	23
1.3.2 Box requirements	24
1.3.3 Database backup and recovery	26
1.3.4 Original ballot protection	27
1.3.5 Web application errors	27
1.4 Integrity	28
1.4.1 Protection against a single point of failure	28
1.4.2 Hardware protections	28
1.4.3 Protection of data input and storage	28
1.4.4 Protection against attempts at improper data entry or retrieval	31
1.4.5 Event recording, logging, and tracking	34
1.4.6 System monitoring	35
1.5 System audit	36
1.5.1 Pre-election audit record	36
1.5.2 System readiness audit record	36
1.5.3 In-process audit records	37
1.5.4 Vote tally data	38



1.5.5	Vote secrecy of DRE systems	38
1.6	Election management system	38
1.6.1	Installing ballots and election-specific programs	39
1.6.2	Testing that ballots and programs are properly installed	39
1.6.3	Generating postvoting reports	39
1.6.4	Processing and producing audit reports	39
1.7	Vote tabulating program	39
1.7.1	Tabulator functions	40
1.7.2	Voting variations	41
1.8	Ballot counter	44
1.8.1	About the Tabulator application	44
1.8.2	Ensuring the counter is set to zero	47
1.8.3	Resetting the counter	47
1.8.4	ScanStation report	48
1.9	Telecommunications	48
1.10	Data retention	48
Chapter 2.	Prevoting capabilities	49
2.1	Ballot preparation	49
2.2	Election programming	49
2.3	Ballot and program installation and control	49
2.3.1	Obtaining the ClearCount software	49
2.3.2	Detailed work plan	49
2.3.3	Software verification	50
2.4	Readiness testing	50
2.5	Verification at the central location	50
2.5.1	Verifying installation and interfaces	51
2.5.2	Verifying the hardware functionality	51
2.5.3	Verifying the software	52



2.5.4	Generating consolidated data reports	52
2.5.5	Segregating test data from actual voting data	53
2.5.6	Test simulation software	53
2.5.7	Testing all ballot positions	53
2.5.8	Verifying equipment readiness	53
2.5.9	Obtaining status and data reports	53
Chapter 3.	Voting capabilities	55
3.1	Verifying ballot-marking devices	55
3.2	Voting booth facility	55
3.3	Secure receptacles for holding voted ballots	55
3.4	Activating a ballot-counting device	55
3.5	Verifying the device	55
3.6	Casting a ballot	56
3.7	Identifying device failure and associated corrective action	56
Chapter 4.	Postvoting capabilities	57
4.1	Closing the polls	57
4.1.1	Shutting down the ClearCount system	57
4.1.2	Shutting down with a planned restart	58
Chapter 5.	Consolidating vote data	59
5.1	How ClearCount consolidates voting data	59
5.1.1	Consolidating data from ScanStations	59
5.1.2	Consolidating data from ClearCast	59
5.2	Producing reports	60
5.2.1	Geographic reporting	60
5.2.2	ScanStation reports	61
5.2.3	Consolidated printed reports	61
5.2.4	Printed reports based on user queries	61
5.2.5	System audit reports	61



5.2.6	Data protection in the reporting process	61
5.2.7	Exporting report data	61
5.2.8	Consolidating polling-place data into a single report	62
5.2.9	Data and report protection	62
5.2.10	Summary of reports created by the ClearCount system	62
5.3	Broadcasting results	62
Chapter 6.	Maintenance, transportation, and storage	63
6.1	Performing routine maintenance	63
6.1.1	Cleaning schedule	63
6.1.2	Cleaning instructions	63
6.1.3	Cleaning materials	63
6.2	Replacing scanner consumables	63
6.3	Performing specialized maintenance	64
6.4	Transportation and storage	64
Appendix A.	Evaluating marks on paper ballots	65
A.1	Vote targets	65
A.2	Ballot layout	66
A.3	Ballot processing by the scanner vendor hardware and software	66
A.3.1	Scanner vendor hardware	66
A.3.2	Scanner vendor software	67
A.4	Ballot processing by the Tabulator application	67
A.4.1	Image grouping	68
A.4.2	Image registration	68
A.4.3	Card identification	68
A.4.4	Mark analysis	69
A.4.5	Vote target classification	71
A.4.6	Result storage	71
A.4.7	Vote target classification diagram	72



A.4.8 Sample ballots	73
A.5 Additional information about ballot mark recognition	75



Preface

This section defines the purpose of this document.

About this document

This document provides an overview of the features and components of the ClearCount system. It corresponds to the *Voluntary Voting Systems Guidelines (VVSG) 2005, Volume 2, Section 2.3* requirements for the technical data package.

Scope of this document

This document contains the following sections:

- Chapter 1. Overall system capabilities
- Chapter 2. Pre-voting capabilities
- Chapter 3. Voting capabilities
- Chapter 4. Post-voting capabilities
- Chapter 5. Consolidating vote data
- Chapter 5. Maintenance, transportation, and storage
- Appendix A. Evaluating marks on paper ballots

Intended audience

This document is intended for state and federal election officials and their voting system test laboratories as part of the technical data package (TDP) required to certify the ClearVote voting system for use. This document is also used by Clear Ballot personnel who support election officials and election staff.

Conventions

This section describes conventions used in this document.

References to ClearVote products

A ClearVote® system can comprise the ClearAccess®, ClearCast®, ClearCount®, and ClearDesign® products. Jurisdictions are not required to purchase all products. You can ignore references to any ClearVote products that are not part of your voting system. Also ignore implementation options that are not relevant to your policies and procedures.

BDF and ADF

ClearAccess imports an election definition contained in an accessible definition file (ADF) created by ClearDesign. ClearCount and ClearCast import an election definition contained in a ballot definition file (BDF) created by ClearDesign.

Versions of ClearDesign earlier than 2.0 created unencrypted ADFs and BDFs. ClearDesign 2.0 and later versions produce encrypted ADFs and BDFs. You can distinguish between unencrypted and encrypted ADFs and BDFs by the ending of the filename.

File type	Filename ends in
Unencrypted accessible definition file	adf.zip
Encrypted accessible definition file	adfx.zip
Unencrypted ballot definition file	bdf.zip
Encrypted ballot definition file	bdfx.zip

In this document, the general terms ADF and BDF can refer to both the unencrypted and encrypted versions of these files.

For the specifics of the ADF and BDF file formats, see the following:

- *ClearDesign Accessible Definition File Guide*
- *ClearDesign Ballot Definition File Guide*

Chapter 1. Overall system capabilities

Responsive to VVSG 2005, Volume 1, Section 2.1.

The ClearCount system is a central-count optical-scan system that runs on unmodified commercial off-the-shelf (COTS) computers and supports specific models of scanners. For a detailed summary of the ClearCount system, see the *ClearCount System Overview*.

The ClearCount system handles the following aspects of the election process:

- Central-count operations
- Vote consolidation

1.1 Security

Responsive to VVSG 2005, Volume 1, Section 2.1.1.

ClearCount security consists of programmatic access control (established via passwords and user access levels), along with physical security. The ClearCount system architecture and recommended methodology integrate to ensure security.

Access control requirements

- When users are created in the ClearCount system, they are assigned a user name, password, and access level. The ClearCount client/server interface is protected by role-based access control lists (ACLs) stored on the CountServer. These ACLs protect the web and MySQL database transactions.
- Network communication is restricted to connections over a closed, wired Ethernet that uses FIPS 140-2 certified encryption. There are no connections to any non-ClearCount computers. There are no wireless or Internet connections. There is nothing in the ClearCount system that requires it to be connected to the Internet for its maintenance, operation, or administration.

Physical control requirements

- The ClearCount system does not modify or damage the ballots in any way.
- The ClearCount architecture ensures that data resides only on the CountServer. (No data is stored on the ScanStations, scanners, or CountStations.)
- The ClearCount system allows a user with the appropriate access level to back up election data and associated card image files and move the backup to a separate computer. This backup can be physically secured by the jurisdiction. It is possible to restore the election to its current state from the backup.

For full details about ClearCount system security, see the *ClearCount Security Specification*.

1.2 Accuracy

Responsive to VVSG 2005, Volume 1, Section 2.1.2.

This section describes the mechanisms by which the ClearCount system ensures and demonstrates the accuracy of its results. ClearCount's accuracy has been tested in Colorado, Florida, Maryland, New York, Ohio, Oregon, Pennsylvania, Vermont, Washington, and Wisconsin. Additionally, Clear Ballot's voting system test laboratory, Pro V&V, conducts independent accuracy testing for state and EAC certifications.

See the *ClearVote Test and Verification Specification* for more information.

1.2.1 Recording contests, candidates, and issues exactly as defined

The ClearVote suite of products offers the ClearDesign election management system (EMS) to create ballot styles and election definitions for import into the ClearCount system.

1.2.1.1 Ballot definition file description and requirements

The ballot definition file (BDF) is a unique file for each election that records all necessary options for casting and recording votes. BDFs enable the ClearCount software to successfully register card images and tabulate vote targets. Registering a card image consists of matching its coordinates to the normalized coordinate system for a specific ballot type.

BDF requirements:

- It uses standard comma-separated values (CSV) format
- It describes the following elements, based on the ballot style PDFs:
 - Ballot style
 - Precinct
 - Each contest name and associated choice names
 - The coordinates of corresponding vote targets

For a full technical description of the BDF, see the *ClearCount Software Design and Specification*.

If the BDF is created by Clear Ballot rather than using the ClearDesign EMS, Clear Ballot tests the BDFs thoroughly as part of its quality assurance process before sending the BDF to the jurisdiction. Upon receipt, the jurisdiction should, in the course of validating a test election, ensure the information in the BDF is accurate.

The criteria that are tested to validate the accuracy of the BDFs are:

- Completeness of ballot style and precincts
- Completeness of contests and choices
- Proper location of contests and choices
- Proper identification of all relevant vote rules

1.2.1.2 ClearCount hardware requirements

The ClearCount system runs on COTS hardware. The requirements for the system are:

- One computer running Ubuntu Linux that acts as the CountServer
- At least one ScanStation computer running the Windows operating system with an attached scanner (of the approved models)
- At least one CountStation running the Windows operating system with an approved browser
- A network switch and cables for the Ethernet network that connects the system
- An optional switch for implementations featuring large numbers of ScanStations

For full details about the hardware used in the ClearCount system, see the *ClearVote Approved Parts List* and the *ClearCount Hardware Specification*.

1.2.1.3 Card image file requirements

The ClearCount system uses card image files created during the scanning process to tabulate results and can retrieve and display these images on demand.

The ClearCount card image files meet the following requirements:

- Each scanned card produces two card image files (one for each side of the card). By default, card images are formatted as industry-standard JPEG images and captured at 200 dpi (dots-per-inch) 8-bit grayscale.
- The Fujitsu PaperStream Capture software creates a unique filename identifier for each card image file. Card images are named with a box ID, a ballot sequence number, and a file extension (for example, AB-004+100004.jpg). The front and back images of each ballot are named sequentially, with the front image bearing an odd number and the back image an even number. The card image files are stored in a folder on the CountServer.
- This specific naming convention ensures reliable Image-to-Ballot Traceability—the ability to locate the physical ballot from which it was captured. The unique card image file identifier is a locator reference that corresponds to the order of the physical ballots.

- Users with the appropriate access level can review all marks on all card image files in the following ways:
 - By paging through the card image files in the Card Images report
 - By tracking image files by combinations of precinct, counter group, or contest
 - By examining a visually annotated version of the card image as described in "Visually annotated card image requirements" on page 21.

These images are used by specific applications for the following purposes:

- The Tabulator application uses them to score and adjudicate vote targets.
- The CountServer serves them in election reports, which are available on demand to users with an access level of read or above following an election.
- They are included in the backup of an election.

1.2.1.4 Election creation requirements

A user with an access level of dbadmin or above can create an election. Creating an election consists of the following requirements:

- The BDF must be imported via a CountStation of the installed ClearCount system.
- On the CountStation, the user logs in to the ClearCount system and chooses **Election Administration** from the login drop-down list.
- On the Election Administration page, the user creates the election by typing a name that identifies the election, navigating to select the BDF, and then clicking **Create Election**.
- The ClearCount software uses the BDF to create and initialize a MySQL database for this election on the CountServer computer.
- The user can verify that the initial database is complete and empty by navigating to the Statement of Votes Cast report and verifying that all appropriate contests and choices are present with zero values. This report can be exported and then printed.
- For instructions about creating elections, see "Creating users and elections" in the *ClearCount Installation Guide*.

1.2.2 Recording votes accurately

The following section provides an overview of how the ClearCount central count system accurately records votes.

The ClearCount vote-recording process consists of the following steps.

1. Cards are scanned on ScanStations. (A ScanStation is a Windows computer, with an attached scanner, that is connected to a CountServer computer via a closed, wired Ethernet.)
2. Scanner software creates image files from the scanned ballot cards.

3. The Tabulator application, running as an instance on each ScanStation computer, counts the ballots and adjudicates the vote for the ballots scanned on that ScanStation. The specific requirements of the different phases of tabulation are described in the subsections below.
4. The results of each Tabulator instance, along with the associated image files, are sent to and consolidated on the CountServer computer.

The ClearCount system divides the population of vote positions as follows:

- Vote targets that have an obvious mark are never incorrectly considered to be a nonvote (or unselected ballot position).
- Vote targets that are clearly empty are never incorrectly considered to be a vote.
- Images with unclear marks or other issues are isolated and flagged for review and resolution.

The full technical specification for the Tabulator application is located in the *ClearCount Software Design and Specification*.

1.2.2.1 Vote tabulation requirements

The Tabulator application is the ClearCount software that processes card images to count the votes for every contest choice. Vote targets and voter marks are adjudicated by the Tabulator instance running on each ScanStation, and then consolidated in the election database on the CountServer, from which results are served as election reports.

Requirements

The Tabulator application:

- Reviews the card images prepared by the scanner software.
- Performs image grouping and image registration (described in "Image registration requirements" on the next page)
- Uses its Discriminant Function module (described in "Discriminant Function requirements" on the next page) to analyze and classify voter marks.

Workflow

The Tabulator workflow consists of the following:

1. An instance of the Tabulator application runs on each ScanStation computer and processes the card images from that scanner.
2. Upon completion of a batch of ballots, the Tabulator application sends its results and the associated card images to the central election database on the CountServer.

For more information about the user interface, see "About the Tabulator application" on page 44.

1.2.2.2 Image registration requirements

This section describes the steps that the Tabulator application performs for image grouping and image registration.

Image grouping requirements

- The Tabulator application processes card image files (which the scanner software places in a folder) asynchronously with the scanner.
- The Tabulator application looks for consecutively named card image files to identify the front and back of the next unprocessed ballot card.

Image registration is the process of determining the logical front of the ballot and its readable orientation, and then locating all important landmarks on the image.

Image registration requirements

- The Tabulator application looks for known identifiable marks on the ballot (the size and location of which vary by voting system). These marks include:
 - Timing marks (edge marks that identify a card's position as it moves through the scanner)
 - Marks in the (EMS-vendor-specific) code channel that identify the ballot style
- The Tabulator application decodes the code channel to determine the card style ID. This is used to determine the layout of vote targets on the ballot.

To pass registration, a card image must meet the following criteria:

- The ballot must scan correctly and produce legible card image files, meaning:
 - It cannot be in a multifeed, where more than one card is pulled into the scanner at once.
 - The resulting images cannot be smeared or occluded by residue from an improperly cleaned scanner.
 - No tears, folds, stains, or stuck-on items can obscure any part of the votable portion of the original ballot.
- The Tabulator must be able to capture the necessary information from the image.

If any of these criteria are not met, the card image fails registration and is digitally outstacked (virtually isolated and placed in a separate category to be resolved later). See "Processing unreadable images" on page 19.

1.2.2.3 Discriminant Function requirements

The Tabulator application uses a module called the Discriminant Function (DF) to analyze the marks read from those card images that pass registration. The DF uses progressive rounds of grouping and comparison to classify voter marks.

Definitions

- **mark**—An obvious human-made mark that indicates voter intent
- **marginal mark**—A human-made mark with some relationship to the vote target such that voter intent is not clear or obvious
- **confidence**—Defined through calculations of vote-target density and zone density

Classification criteria

- The darkness of the mark.
- How completely it fills the vote target.
- Whether the mark fits the pattern used by this voter on other contests on the same card.

Analysis and scoring steps

The DF does the following:

1. Assigns a vote target score of 0 to 100 based on the darkness of the mark on the vote target.
2. Performs a noise floor calculation, where it calculates the relative darkness of the paper stock and variations in lighting conditions between the two cameras in the scanner.
3. Successively applies three functions over the population to properly classify vote targets:
 - a. Divides the population based on whether each mark is sufficiently above the noise floor.
 - b. Compares the vote targets in each contest to one another to determine which might represent stray marks.
 - c. Compares the vote targets across the card to accommodate various voter mark styles.

1.2.2.4 Vote target classification requirements

The next step in the ClearCount system is vote target classification.

- The system applies the voting rule for each contest to the marks for that contest.
- It reviews human-marked vote targets and assigns them as votes, overvotes, undervotes, or nonvotes (or unselected ballot positions).

1.2.2.5 Audit logging requirements

The ClearCount system logs every human action, as well as all scanning and tabulating actions. For a description of ClearCount logging, see "Event recording, logging, and tracking" on page 34.

1.2.2.6 Processing unreadable images

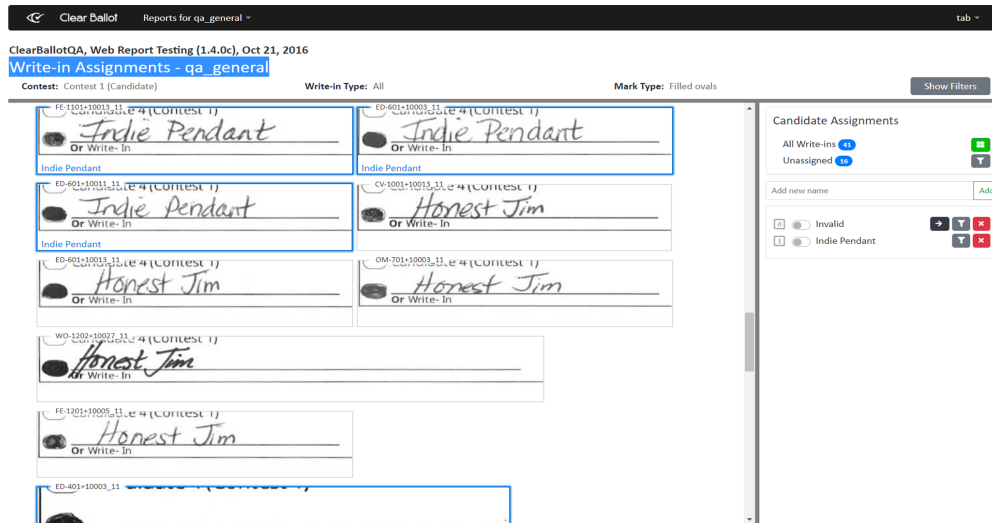
If, for any reason, one or both of the images associated with a card fail registration, a record is written to the election database indicating the date, time, and failure code. Cards whose image files fail registration are flagged and virtually isolated in a process called *digital outstacking*. These cards must go through *digital resolution* using manual adjudication for their results to be included in the totals. Digital resolution can only take place when the election is not in the Closed phase.

A user with an access level of modify or above, using a CountStation, can access these card images from the Dashboard by clicking the number associated with the Unreadable Card Images Needing Resolution. This links to the Card Resolutions page, where the election official can launch the Card Resolutions tool.

Requirements for processing unreadable card images

- Card images must pass registration to be automatically classified, counted and reported.
- Card images that do not pass registration are virtually isolated and digitally outstacked.
- Obscured card images do not pass registration. Conditions can include:
 - Multifeeds
 - Tears, folds, or creases
 - Stains or barriers that prevent scanner observation of marks, contests, or timing marks
- Images that fail registration are written to the election database with the date, time, and failure code.
- Digitally outstacked cards are listed in the Dashboard's Visual Resolution of Unreadable Cards section. Clicking the number associated with the Unreadable Card Images Needing Resolution heading opens the Card Resolutions page. From there, the user can click a card ID in the Unresolved Cards table to open the Card Resolutions tool.
- Users with an access level of modify or above can access digital images from the Dashboard on the CountStation.
- The number of unreadable card images needing resolution is reported on the Dashboard. When a user with modify access level or above clicks the number, the Card Resolutions page appears. (If a user with a lower access level, such as read, clicks the number, he or she sees the Card Images report instead, which is not user-editable.)

The Card Resolutions report is described in the *ClearCount Reporting Guide*. The "Resolving card tabulation issues" section of the *ClearCount Election Administration Guide* describes the Card Resolutions tool.



1.2.2.8 Visually annotated card image requirements

The ClearCount system produces a visually annotated version of each card image that can be used for human confirmation of the accuracy of system results on a per card basis.

The system allows any user with read access or above to access the visually annotated version of a card image by navigating to the Dashboard for that election, clicking the number of **# Pages Scanned (Ballots and Nonballots)**, clicking the card image you want to review, and then clicking **Show visually annotated card identifier**.

An annotated version of the card image appears, with each vote target outlined in red and the text for the winning choice in green.

Requirements

- The CountServer displays the Dashboard as a browser page.
- From the CountStation, following the close of polls, any user with read access or above can access the Card Images report by clicking the number associated with the **# Pages Scanned (Ballots and Nonballots)**.
- This user selects the card image to review by clicking that image in the Card Images report.
- On the Card Information page that displays, the user can click **Show visually annotated card identifier** to see the visually annotated version of the ballot.

		STATE	NONPARTISAN
<p>TO VOTE, COMPLETELY FILL IN THE OVAL NEXT TO YOUR CHOICE.</p> <ul style="list-style-type: none"> Use only the marking device provided or a black ink pen. If you make a mistake, don't hesitate to ask for a new ballot. If you erase or make other marks, your vote may not count. To vote for a candidate whose name is not printed on the ballot, fill in the oval, and write in the candidate's name on the blank line provided for write-in candidate. 			
		CHIEF FINANCIAL OFFICER	Shall Justice Paul M. Hawkes of the First District Court of Appeal be retained in office?
		CHIEF FINANCIAL OFFICER (Vote for One)	
<input checked="" type="radio"/>	Jeff Atwater	REP	<input checked="" type="radio"/> YES
<input type="radio"/>	Loranne Ausley	DEM	<input type="radio"/> NO
<input type="radio"/>	Ken Mazzie	NPA	<input type="radio"/> NO
<input type="radio"/>	Tom Stearns	NPA	
		COMMISSIONER OF AGRICULTURE	Shall Justice Charles J. Kahn, Jr. of the First District Court of Appeal be retained in office?
		COMMISSIONER OF AGRICULTURE (Vote for One)	
<input checked="" type="radio"/>	Adam H. Putnam	REP	<input checked="" type="radio"/> YES
<input type="radio"/>	Scott Maddox	DEM	<input type="radio"/> NO
<input type="radio"/>	Ira Chester	TEA	
<input type="radio"/>	Thad Hamilton	NPA	
		LEGISLATIVE	Shall Justice Phil Padovano of the First District Court of Appeal be retained in office?
		LEGISLATIVE	<input checked="" type="radio"/> YES
		LEGISLATIVE	<input type="radio"/> NO
		STATE REPRESENTATIVE DISTRICT 6 (Vote for One)	Shall Justice Lori S. Rowe of the First District Court of Appeal be retained in office?
<input checked="" type="radio"/>	Jimmy Patronis	REP	<input checked="" type="radio"/> YES
<input type="radio"/>	John McDonald	DEM	<input type="radio"/> NO
<input type="radio"/>	John McDonald	DEM	<input type="radio"/> YES
		COUNTY	<input type="radio"/> NO

Figure 1-2. Example of visually annotated card

1.2.3 Producing accurate, detailed reports

The ClearCount system generates a set of election reports that are served as browser pages created from the Tabulator data in the election database.

See the *ClearCount Reporting Guide* for report descriptions.

Requirements

- Election reports are displayed as pages in a browser on the CountStation.
- The ClearCount web server process on the CountServer controls the display of reports.
- Election reports can be accessed by users with read access level or above from a browser on a CountStation. Vote totals may not be visible on reports if the election administrator has disabled access to vote totals, which is typically done prior to the close of polls on Election Day.
- As with any other user action, accessing reports is logged to the system's web activity log and election activity log.
- The ClearCount system contains no custom query functionality. On many reports, users can configure certain elements of display, such as filtering and the number of items shown per page.

Although the term *tabulation* is used throughout this and related ClearCount documents to refer to both processing voter marks on a ballot and producing results reports, the ClearCount system does *not* actually tabulate any results into human-readable information unless and until an authorized user requests a results report. In other words, the actual tabulation of a set of ballots occurs on request in real time and not until that time.

The ClearCount election reports allow users to access any of the relevant links or images. To confirm the accuracy of these reports, election officials can manually check the tallies.

To ensure the accuracy of its reports, the ClearCount system uses two election identities to ensure contest and candidate adjudication is made.

- The Contest Election Identity states that for each contest on a ballot, that contest must be classified as either being properly voted, blank-voted, or overvoted. The number of ballots in each of these classifications must equal the total number of ballots on which that contest is present. This prevents contests from being overlooked by the system and allows the user to easily verify that each ballot has been classified.
- The Choice Election Identity states that for each choice within a contest on a ballot, that choice must be classified as a vote, as a nonvote, or as participating in an undervote or an overvote. As with the Contest Election Identity, this means that the total of votes, overvotes, undervotes, and nonvotes for a given choice must equal the total number of times that the choice appeared on a scanned card.

1.3 Error recovery

Responsive to VVSG 2005, Volume 1, Section 2.1.3.

The ClearCount system includes several features that aid in error recovery. It is constructed to ensure errors are not introduced into the system due to hardware, power, or connection issues. The system stores all data in protected databases to prevent data corruption.

1.3.1 System and software errors

In the ClearCount system, cards are identified and scanned by box. This apportioning helps any errors surface quickly.

1.3.2 Box requirements

- The ClearCount system processes cards by the box.
- Each box is labeled and identified by one or more box ID labels and target cards, as follows:
 - In most cases, all of the cards in a box are part of the same batch and can be identified by the same target card and box label.
 - Occasionally, a scanner operator may accidentally cancel a batch when trying to clear a paper jam. In this case, the user can use a new target card for the remainder of the cards in the box and add a second corresponding box ID label.
- Box ID label and target card requirements:
 - Box ID labels and target cards are required by the ClearCount system.
 - A box ID label physically identifies each box and its corresponding cards. The box ID naming scheme consists of an abbreviation for the counter group of the cards in the box (such as ED for Election Day), as well as a box sequence number (for example, ED-001).
 - A box ID label must be affixed to the outside of the ballot box and should be consistently placed in the same location (such as the upper right corner) to aid in quickly identifying ballot boxes.
 - A target card identifies the cards in a batch or box to the scanner. (It is similar to the header card used in other election systems.)
 - The ID on the target card for a box must match the ID on the box label.
- Card image identifier requirements:
 - A card image's identifiers are a combination of the box ID and image sequence number.
 - When a card is scanned, the front and back images are each given a unique identifier (such as ED-001+00001 and ED-001+00002) corresponding to the batch or box ID (ED-001) and image file (+00001 or +00002).
 - This unique identifier is used for Clear Ballot's Image-to-Ballot Traceability feature. During the election verification process, this gives election officials the ability to locate a physical card for manual review and resolution if necessary.
- At the beginning of scanning a box, the Tabulator application issues a message when it identifies the target card. If cards are scanned without a target card, the system does not recognize the card images as such and the Tabulator application cannot process them.
- Clear Ballot provides jurisdictions with PDF file versions of the target cards and box labels that can be downloaded from the Clear Ballot website and printed on-site prior to the scanning process. There are a number of different target and label PDF files based on the counter groups used in an election. For full documentation of this process, see "Target cards and box labels" in the *ClearCount Installation Guide*.

1.3.2.1 Box deletion requirements

The ClearCount system includes a box deletion feature that allows an authorized election official to erase card image files and associated data on a box-level basis and then rescan the box. Box deletion and rescanning can address human error (such as accidentally scanning a batch of cards twice) or technical errors (such as scanner multifeeds or misfeeds).

Requirements for deleting a box

- Card image files cannot be deleted individually. Deletion of card images requires the deletion of an entire ballot box.
- A box must be deleted from the ScanStation where it was originally scanned if that computer is still functioning. If the computer has crashed, the box can be deleted remotely from a CountStation. Both of these procedures are described in "Troubleshooting scanning issues" in the *ClearCount Election Administration Guide*.
- Before deleting a box, the Tabulator instance running on that ScanStation must be closed.
- Box deletion is limited to users with an access level of modify or above. Users who do not have this level of access cannot delete a box.
- To control access, when a user double-clicks the DeleteBox.bat file, a user name and password dialog appear. Users who lack the proper access level cannot log in.
- After logging in, the authorized user can select the box in question and press the Enter key. This deletes all saved images and election database entries from the box on the ScanStation and on the CountServer.
- Deletion of the box is logged by user and time to the election activity log.
- For full details of box deletion, see "Troubleshooting scanning issues" in the *ClearCount Election Administration Guide*.

Causes for deleting a box

- Loss of target card identity by the scanner. (If this situation occurs partway through scanning, it might instead be addressed by adding a new target card and box ID label to the box.)
- Human errors, including cards getting out of order or the scanner operator accidentally terminating the Tabulator application before all of the ballots in a box have been scanned.
- Multifeeds resulting in image files containing more than one card.
- After resolving an unvotable card in the box.
- Fatal Tabulator errors (appearing in red on the Tabulator console, as well as being logged to the election activity log) are described in "ClearCount messages" in the *ClearCount Election Administration Guide*.

1.3.2.2 Audit logging locations

All ClearCount system and software events, and errors are logged to the following locations:

- The ClearCount web activity log tracks all users' web-based actions for all of the jurisdiction's elections. This includes CountServer, ScanStation and CountStation logins, logouts, and authentication failures; user access to election reports and card images; ballot card resolution; and administrative changes to elections and users.
- The ClearCount election activity log tracks events in a specific election, including user access to election reports and logs; as well as Tabulator start, processing, and end events; probable target card and scanning error identification; and CountServer warning and error messages. The election activity log also tracks overall scanning rate and progress across ScanStations.
- The Windows Event Log on each ScanStation and CountStation logs all operating system-specific actions on each respective computer.
- The CountServer, which is Linux-based, is configured as an appliance. After installation, under normal use, there is no need for any direct access to the CountServer. Remote access to the CountServer is logged to the ClearCount web activity log.

For a full description of the functional requirements for the ClearCount activity logs, see "Event recording, logging, and tracking" on page 34.

For user documentation on these logs, see "ClearCount log files" in the *ClearCount Election Administration Guide*.

For a list of ClearCount warning and error messages and how to respond to them, see "ClearCount messages" in the *ClearCount Election Administration Guide*.

1.3.3 Database backup and recovery

The ClearCount system includes the ability to back up an election and related card images to an external hard drive that can then be physically secured by a jurisdiction.

Backup and recovery requirements

- During central-count scanning, jurisdictions must back up the election on a daily basis. They can choose to back up more frequently.
- Users with an access level of dbadmin or above can back up the election and related card images.
- This backup must be copied to an external hard drive that must then be physically secured by the jurisdiction.
- Users with an access level of dbadmin or above can restore the election from this backup.
- Backup and restore actions are performed via the Election Administration pages on a CountStation.

- Procedures for election backup and recovery are described in "Managing elections" in the *ClearCount Election Administration Guide*.

1.3.4 Original ballot protection

The presence of the original ballots provides an additional layer of disaster recovery protection.

Original ballot protection requirements

- The original ballots are not damaged or changed in any way by the ClearCount scanning process.
- The ballots must be maintained within their boxes in the order in which they were scanned. This allows individual ballots to be located after scanning.
- After scanning, ballots must be stored according to jurisdictional statutes.
- As documented in the ClearCount user manuals and security specification, secure storage and preservation of the voted, scanned cards in the order of scanning with the appropriate box ID and target card is a required backup process.

1.3.5 Web application errors

The ClearCount system uses a closed, wired Ethernet network. There are no Internet connections.

Browser-based applications in the ClearCount system include the following:

- Election reports
- Election Administration pages
- User Administration pages
- Card Resolutions tool

If a user clicks a link or enters a correct URL and it does not take the user to the expected location, this indicates a bug in the ClearCount software. The system displays an error message. The error is logged in the election activity log and should be reported to Clear Ballot Technical Support.

Error message requirements

- ClearCount error messages include date and timestamp information, the source of the error, the severity, and a description.
- Information about error correction actions appears in "ClearCount messages" in the *ClearCount Election Administration Guide*.

1.4 Integrity

Responsive to VVSG 2005, Volume 1, Section 2.1.4.

This section describes the physical and functional integrity measures that ensure the stability and function of the vote capture and counting process of the ClearCount system.

1.4.1 Protection against a single point of failure

Because the ClearCount system is not a precinct-count system, it does not run in the polling place. Therefore, the requirement that it protect against a single point of failure that would prevent further voting at the polling place does not apply.

1.4.2 Hardware protections

All of the hardware that the ClearCount system uses is unmodified COTS hardware that has been developed and tested to protect against physical threats, such as interruption of electrical power, generated or induced electromagnetic radiation, and ambient temperature and humidity fluctuations.

To ascertain that the COTS hardware used in the ClearCount system meets the requirements set out by the (VVSG), Clear Ballot obtained and examined copies of the manufacturers' specifications and documentation. The ClearCount TDP contains copies of manufacturers' documentation demonstrating protection details.

Each piece of COTS hardware used in the ClearCount system has an FCC Class B certification, a CE mark, and a UL or other safety mark affixed to it. Some accessory items may carry only FCC Class A electromagnetic interference limits.

The *ClearVote Quality Assurance Program* describes the process by which Clear Ballot has verified the COTS development and testing that protects the system against physical threats.

For specific details about hardware protections, see the *ClearCount Hardware Specification*.

1.4.3 Protection of data input and storage

Because the ClearCount system is a central-count system, it does not have the same time constraints as a precinct-count system. If any data input or storage device malfunctions, election officials can repair the device or replace it with a backup version that is either readily available or obtained later.

All replacement equipment must undergo full testing in compliance with applicable regulations, as documented in the *ClearCount Installation Guide*.

Data input by scanner

Data input by scanner is protected against failure by the following mechanisms:

- In a multiscanner setup, several scanners are networked together. If a single scanner fails, other scanners in the network can continue to scan ballots.
- In a single-scanner setup, if the scanner fails, the jurisdiction must repair or replace the scanner.
- Clear Ballot strongly encourages each jurisdiction to enter into a service contract with the scanner manufacturer. In case of failure, the jurisdiction's scanner service contract ensures the restoration of scanner service (via repair or replacement) within a specified time.
- Jurisdictions that want to have scanner technicians available for on-site repairs must enter a separate maintenance agreement with the scanner manufacturer. Service agreements are individually negotiated between the jurisdiction and the scanner manufacturer. Services offered by the scanner manufacturer may vary based upon location and other factors relevant to the individual jurisdiction.

ScanStation failure

The effect of a failed ScanStation on the ClearCount system is as follows:

- After scanning and adjudicating each box of ballots, the card image files and associated adjudication data are pushed from the ScanStation to the CountServer, where they are consolidated with other results. If a CountStation fails, only the current box of ballots is affected. The jurisdiction only needs to delete that box and rescan the ballots on a different ScanStation.
- In the ClearCount system, ballots are scanned and adjudicated on a per box basis and the card images and election data are immediately sent to the CountServer. All consolidation and storage takes place on the CountServer. A ScanStation has no interaction with other ScanStations. Nothing that happens on one ScanStation has any impact on other ScanStations.
- A backup ScanStation can be added to the network during an election. The addition of a ScanStation is recorded as follows:
 - Whenever a new ScanStation is attached, election officials must run an update script that pulls the scanner's serial number from the scanner and enters it in the election activity log.
 - The Card Inventory Report lists which ScanStation scanned each box of ballots.
 - The ScanStation Report lists the start and stop time of each scanner.
- A failed ScanStation that is part of a multiscanner network can remain connected to the network during an election count without causing a loss of votes or any other disruption.
- The presence of a failed ScanStation on the network does not affect the function or performance of other ScanStations.

Stored data

The ClearCount results and card image files are stored in a centralized database that resides on the CountServer as soon as adjudication of each batch of ballots is complete. No data is stored on a ScanStation computer.

After tabulation, election data can be backed up to an external hard drive, as well as exported or printed. The election data, including the card image files, can be restored from the backup. ClearCount guidelines require that data be backed up at the end of each day of tabulation, but jurisdictions can back up their data more frequently.

The backup and restore processes are launched from the Election Administration page on a CountStation to an external hard drive.

Stored data requirements

- Card image files and election results are written to the election database on the CountServer at the time they are scanned and adjudicated. No data is left on the ScanStation after the Tabulator application has finished its run.
- All ScanStation activity, after a ScanStation begins scanning, is logged to the central database on the CountServer.
- If the CountServer fails, jurisdictions can revert to the backup taken at the end of the previous day. They only need to rescan the ballots from the point of the latest backup.
- Election results data is viewable in the form of election reports. These reports can be viewed on a CountStation by any user with read access or above, as follows:
 - As governed by statute, prior to the close of polls on Election Day, reports that contain vote counts or card images cannot be viewed by anyone.
 - Prior to Election Day close of polls, no vote counts are displayed, although the rest of the information on the web page is displayed.
 - In addition, users with an access level of modify or above can begin resolving unreadable ballots in the Card Resolutions tool prior to the close of polls.
 - After the close of polls, users with an access level of read or above can view all vote totals.

Election backup and restoration requirements

- The system provides the ability to back up an election on demand. The election can be completely restored to its current state from the backup.
- This backup includes both tabulation data and the scanned card image files. To back up an election, either during the scanning process or after the election is complete, a user with dbadmin access level or above can log in to a CountStation, select the **Election Administration** option and select the **Back Up Election** option. For full details, see "Backing up an election" in the *ClearCount Election Administration Guide*.
- The election data is copied to an external hard drive.

- To protect against loss of power, the ScanStation computers used in the ClearCount system feature battery backup. The scanners do not store any data. If a scanner loses power while scanning a box of ballots, the scanner operator should have a supervisor delete the box and then rescan it.

Ballot-level protection requirements

- The ClearCount system does not damage or alter original ballots.
- Clear Ballot's Image-to-Ballot Traceability feature in the ClearCount system labels card image files with an ID that corresponds to the ID on the ballot box and the ballot's position within the box. Any individual ballot can be retrieved without difficulty (as long as ballots have been kept in order as required by ClearCount procedures). To track a paper ballot from an image file, follow the instructions in "Scanning for a specific card" in the *ClearCount Election Administration Guide*.

1.4.4 Protection against attempts at improper data entry or retrieval

Improper data entry and retrieval are prohibited through numerous mechanisms.

When a user is created in the system, he or she is assigned a user name and a password. Access to the system requires logging in with the user name and password. The ClearCount system times out user login sessions after 24 hours of inactivity or when the CountServer is restarted, whichever occurs first. All user actions, including viewing election reports, are logged by user name and machine name.

A user who tries to log in with an incorrect password receives a *login failed* message and is not allowed to access the system. A warning message detailing the failed login attempt is logged to the web activity log. (Because it is not associated with a particular election, it is not logged to the election activity log.)

The system does not allow passwords to be recovered, but they can be reset by a user with an access level of useradmin if they have been lost or compromised.

1.4.4.1 User name and password requirements

User name and password requirements include the following:

- User names and passwords must be all ASCII characters.
- User names can be up to 16 characters long.
- For ease of use, Clear Ballot recommends all lowercase characters for user names.
- Clear Ballot recommends that, for identification purposes, user names be based on the user's real name rather than on his or her role.
- Passwords can be from 1 to 128 characters long.
- Passwords should consist of a mix of uppercase and lowercase letters and numbers.
- For full ClearCount password guidelines, see the *ClearCount Security Specification*.

1.4.4.2 Access control requirements

Each user in the ClearCount system is assigned an access level that controls his or her permissions on the system. Users are assigned this access level at the time they are created. User access levels can be changed by a user with the access level of `useradmin`.

Access levels are hierarchical, meaning that each successive level encompasses the permissions of previous levels. Access levels include:

- **useradmin**—Can manage ClearCount user accounts (adding, modifying or deleting users) and passwords, and can do anything the following levels can do.
- **dbadmin**—Can manage ClearCount election databases (add or delete elections, back up and restore elections, set the active election, change the election phase, and merge ClearCast results), and can do anything the following levels can do.
- **modify**—Can resolve unreadable cards digitally and delete boxes of ballots and can do anything the following levels can do.
- **append**—Used for ballot scanning. Can add new ballot processing results and log events. Can use HTTPS to send card image files to be stored on the CountServer. This is the access level assigned to ScanStations.
- **read**—Can view reports and activity logs. Cannot modify any part of the election database.
- **none**—No access allowed at all. This setting can be used to temporarily deactivate a user account without deleting it.

For full details about ClearCount access control, see the *ClearCount Security Specification*.

1.4.4.3 Data input protection

Scanner operators only have access to their individual ScanStations and not to the CountServer where image file data is stored. Scanner operators are limited in what they can access from their ScanStations. They can monitor the Tabulator application's progress on the computer screen, but they cannot view card images, vote counts, election reports, or any information from another ScanStation.

The Tabulator window on each ScanStation does not share any election results. It displays only a high-level view of ballot processing and any related errors, including:

- Scanning, adjudicating, and image-saving statuses
- The number of boxes and ballots completed
- The number of ballots with errors and the error rate
- The scanning speed

1.4.4.4 Requirements for resolving unreadable ballot cards

When the ClearCount system encounters a card image that it cannot resolve, it *digitally outstacks* it. That is, the ClearCount system includes the card in the tally of unreadable card images needing resolution. These images appear in the Card Resolutions tool, which election officials can use to review and, when appropriate, resolve the unreadable card images. This tool is only available to users with modify access or above, and like every other user action, is logged by user name and computer name or IP address. For more information about the Card Resolutions tool, see "Processing unreadable images" on page 19.

To locate a paper card from an image file, see "Scanning for a specific card" in the *ClearCount Election Administration Guide*.

1.4.4.5 Scanner safeguards on single card-feed functionality

The scanners used in the ClearCount system contain an ultrasonic sensor that vibrates the edges of the cards to detect if more than one card is being pulled through the scanner at the same time. If a multifeed is detected, the ScanStation issues a message and stops. The scanner operator can separate and properly rescan the cards in question. For full documentation of the related scanner error messages and the procedures to resolve them on different scanner models, see the *ClearCount Maintenance Guide*.

For best scanning results, consult the *ClearVote Ballot Stock and Printing Specification* for recommended paper stocks.

1.4.4.6 Control over access to election results

Upon completion of the scanning process, the ClearCount system allows stakeholders with the appropriate access level to view election reports via the CountStation. Only users with the appropriate access level can track progress during the election (by monitoring the Dashboard's Election Data and Ballot Scanning Operations sections) and, after the election, view the election results.

Requirements for access to election results

- The reports are served from the election database on the CountServer that users with a read access level or above can access from a CountStation.
- Vote totals may not be visible on reports if the election administrator has disabled access to vote totals, which is typically done prior to the close of polls on Election Day.
- All reports are read-only. Users cannot change the results in the election database.
- Users viewing reports can filter results, resize images, and set the number of results to be displayed on a single page.
- A description of each report and its contents can be found in the *ClearCount Reporting Guide*.

1.4.4.7 Requirements for physical security between elections

Between elections, Clear Ballot policy requires that the jurisdiction lock down the CountServer, ScanStations, CountStations, and other hardware so no third-party access or software can affect their security. This ensures that the integrity of the hardware is not compromised between elections.

1.4.5 Event recording, logging, and tracking

The ClearCount logging system tracks all user and system actions in logs: a single web activity log and an election activity log for each election. The ClearCount logs are accessed as browser pages on a CountStation, which is connected to the CountServer via a closed, wired Ethernet.

This section summarizes the requirements for these logs. For user documentation, see "ClearCount log files" in the *ClearCount Election Administration Guide*.

1.4.5.1 Web activity log

The ClearCount web activity log tracks all users' web-based actions for all of the jurisdiction's elections. This includes CountServer, ScanStation and CountStation logins, logouts, and authentication failures; user access to election reports and card images; ballot card resolutions; and administrative changes to elections and users. See "Web activity log" in the *ClearCount Election Administration Guide* for details.

Requirements

- The web activity log is accessed from the ClearCount login drop-down menu. (The number of items on this menu varies depending upon the user's access level.)
- Users with a read access level or above can view the log.
- The log is read-only and cannot be modified by any user.
- Normal and abnormal events are logged.
- The web activity log is stored as a separate record in the election database.
- The web activity log can be printed or exported by users with read access level or above.

1.4.5.2 Election activity log

For each election, the ClearCount system generates a separate election activity log. This log resides as a separate record with its election in the database.

Along with tracking user actions for the election, the election activity log lists the Tabulator application's start, processing, and end events; probable target card and scanning error identification; and server warning and error messages. Each Tabulator instance is identified by the machine name of the ScanStation computer that is running the process. The election activity log also tracks overall scanning rate and progress across ScanStations. See "Election activity log" in the *ClearCount Election Administration Guide* for details.

Election activity log requirements

- The election activity log is accessed from the Reports drop-down menu.
- Users with a read access level or above can view, print, or export the log.
- The log is read-only and cannot be modified by any user.
- Normal and abnormal events are logged.
- The election activity log is for a specific election.
- The election activity log is backed up and restored with its election.
- The election activity log cannot be deleted from the election database.

An election that has been backed up can be deleted from the CountServer. That action deletes the associated election activity log.

1.4.5.3 ClearCount log storage, backup, and access

For both the web activity log and the election activity log, each logged event is stored as a separate record in the database. If an election is deleted, its election activity log is preserved in the backup. If the election is restored from backup, the election activity log entries are restored as well. Both logs can be printed or exported like any ClearCount election report.

1.4.6 System monitoring

The ClearCount software uses system monitoring on its Linux CountServer and its Windows ScanStations and CountStations. For complete details about system monitoring, see "Validating and securing the system" in the *ClearCount Installation Guide*.

1.4.6.1 Linux system monitoring

The CountServer creates a default Linux administrative account during installation. As documented, this account should be used only if the jurisdiction is instructed to do so by Clear Ballot Technical Support for debugging purposes. This account is not required or used for normal electoral tasks.

The ClearCount web activity log captures events related to the CountServer, including a user opening or closing a session or any authentication failure. To monitor CountServer access in the web activity log, the user sorts on the Source column and looks for Linux entries.

For information about viewing Linux log files, see <https://help.ubuntu.com/community/LinuxLogFiles>.

1.4.6.2 Windows system monitoring

To ensure ScanStations and CountStations are secured against unauthorized access and improper program installation, the ClearCount system uses native Windows system monitoring tools, such as the Windows Event Log. For a full description of how these tools are implemented, see "Validating and securing the system" in the *ClearCount Installation Guide*.

1.5 System audit

Responsive to VVSG 2005, Volume 1, Section 2.1.5.

This section provides a functional description of the system audit capabilities of the ClearCount system.

1.5.1 Pre-election audit record

Responsive to VVSG 2005, Volume 1, Section 5.4.1.

The ClearDesign EMS handles election definition and ballot preparation. See the ClearDesign documentation for more information.

1.5.2 System readiness audit record

Responsive to VVSG 2005, Volume 1, Section 5.4.2.

This section describes the ClearCount system readiness audit record.

- Prior to ballot counting, election officials can verify hardware and software status as part of ClearCount readiness testing (which is documented in "ClearCount readiness testing" in the *ClearCount Installation Guide*). The backup taken of the test election, including its election activity log, serves as the system readiness audit record. In addition, the active election is logged in the web activity log, which spans all test and actual elections run by the jurisdiction.
- System readiness is logged to the election activity log with the following messages: "Scanner *modelAndSerialNumber* connected" and "ClearCount *versionAndReleaseDate* Tabulator Started."
- Polling place identification: Because the ClearCount system does not have a polling-place element, it does not address this requirement.
- ClearCount readiness testing tests and records the correct installation of ballot formats on its system. As part of readiness testing, election officials must run at least one ballot of each ballot style, review the vote visualizations in the election reports, and make sure that candidates and contests are displayed correctly. If any bugs are identified, the jurisdiction works with Clear Ballot to correct the BDF, following which they repeat the readiness testing exercise and review.
- The requirement that the software check and record the status of all data paths and memory locations to be used in vote recording to protect against contamination of voting data is not applicable to the structure of the ClearCount software, so this document does not address this requirement.
- After running the test election, a user with dbadmin access level or above should back up and then delete the test election. In the web activity log, the delete action is logged with the user name and time stamp and the following messages: "Database *electionName_test* deleted" and "Image folder *pathToTestElection/electionName_test* deleted."

- The number of cards scanned during readiness testing is determined by jurisdictional statute. (ClearCount does not support simulated testing. Jurisdictions must scan actual ballots as part of their testing.) Election officials should run the test ballots, examine results in the election reports, and not go forward until any problems are resolved.
- Public network report: Because the ClearCount system does not use a public network, this document does not address this requirement.

1.5.3 In-process audit records

The ClearCount system logs system and user operations during the scanning and tallying of cards. The first message that is written to the web activity log shows the initial user logging in to the Linux CountServer. Subsequently, the web activity log captures election and user creation and user login, logout, and use of the ClearCount web applications.

The ClearCount system generates event, error, and exception messages for its software components, as follows:

- The Tabulator application writes messages to its terminal screen, as well as to the election activity log for the election. The initiation and termination of each ScanStation's instance of the Tabulator application and its associated scanner are logged to the election activity log. For explanations of Tabulator error messages and suggested responses, see "ClearCount messages" in the *ClearCount Election Administration Guide*.
- The User Administration and Election Administration pages and election reports write messages to the web activity log. For explanations of error messages and suggested responses, see "ClearCount messages" in the *ClearCount Election Administration Guide*.
- The ScanStation logs messages in the following ways:
 - When a ScanStation is started or stopped, the action is logged to the Windows log.
 - Scanner and scanner software errors are logged to the election activity log. Documentation covering scanner error and exception information can be found in the manufacturer's documentation, which is included with the TDP submission.
 - In the event of a power failure, an unexpected restart is written to the Windows Event Log.
 - CountServer session opening and closing are logged to the web activity log.
 - Transmission errors, memory errors, or problems saving files are written to the web activity log. For example, if a user rescanned a previously scanned box, the system writes an alert to the web activity log.

The ClearCount zero report consists of a Statement of Votes Cast report that is generated after the election is created, but before scanning cards begins. This version of the report shows all candidates and questions with zeroes in all vote positions.

1.5.4 Vote tally data

Responsive to VVSG 2005, Volume 1, Section 5.4.4.

The ClearCount system contains the following features for reporting results and verifying an accurate count.

- The number of cards cast, using each ballot configuration, by ScanStation, by precinct, and by political subdivision, is included in the ClearCount election reports, which are described in the *ClearCount Reporting Guide*.
- Candidate and measure vote totals for each contest, by ScanStation, are included in the ClearCount election reports.
- The number of ballots read within each precinct are included in the ClearCount election reports. For primary elections, separate totals are provided for each party.
- The ClearCount system provides separate tallying of votes, overvotes, undervotes, and nonvotes for each contest, by ScanStation, precinct, and additional jurisdictional levels.
- The number of cards able to be processed and unable to be processed, as well as the total number of cards read, are displayed on the election's Dashboard.

1.5.5 Vote secrecy of DRE systems

Because the ClearCount system does not include a DRE component, this document does not address the vote secrecy of DRE systems.

1.6 Election management system

Responsive to VVSG 2005, Volume 1, Section 2.1.6.

Election officials use the ClearDesign EMS to create ballots and to generate the election definition.

The ClearCount system covers the following aspects of election management:

- Installing ballots (in the form of a BDF for each election) and the ClearCount software
- Testing that its BDF and software programs have been properly prepared and installed
- Tabulating the vote
- Generating post-voting reports, in the form of ClearCount election reports

The following sections discuss each of these aspects.

1.6.1 Installing ballots and election-specific programs

The ClearCount software is distributed on DVD. The software, along with the Linux operating system and all required software dependencies, is installed only on the CountServer. The installation overwrites the existing operating system, along with any other software on that computer.

The product documentation is distributed on a DVD and can be installed on any Windows computer. Detailed instructions about installing the ClearCount software and creating an election can be found in the *ClearCount Installation Guide*.

While the ScanStations have a few software dependencies (such as the software required for the scanner hardware), all ClearCount software that runs on client computers is read at run time from files residing on the CountServer. The ClearCount software is only installed on the CountServer.

To create an election in the ClearCount system, a user with a dbadmin access level or above uses a CountStation to import the BDF created from the jurisdiction's ballot style PDFs.

1.6.2 Testing that ballots and programs are properly installed

Detailed instructions about performing readiness testing on the installed ClearCount system can be found in the *ClearCount Installation Guide*.

1.6.3 Generating postvoting reports

The ClearCount system generates postvoting reports that do the following:

- Support geographic reporting
- List the number of cards counted by each ScanStation
- Produce a Statement of Votes Cast for each contest
- Provide exportable reports that can be printed or distributed electronically
- Prevent data from being altered or destroyed by report generation or transmission

For more information, see the *ClearCount Reporting Guide*.

1.6.4 Processing and producing audit reports

The ClearCount web activity log and election activity log provide an audit log of all user and Tabulator actions. These logs can be copied, printed, or exported in CSV format, as well as viewed in a browser on a CountStation. The election activity log is included in the backup of the election.

1.7 Vote tabulating program

Responsive to VVSG 2005, Volume 1, Section 2.1.7.

The ClearCount system's vote tabulation program, the Tabulator application, is described in the following section.

1.7.1 Tabulator functions

Responsive to VVSG 2005, Volume 1, Section 2.1.7.1.

An instance of the Tabulator application runs on each ScanStation. The ClearCount system scans ballots into electronic image files, analyzes them, and sends the results to a centralized database on the CountServer. The following sections describe the Tabulator functions.

1.7.1.1 Monitor system status and generate machine-level audit reports

The ClearCount system monitors system status and generates audit reports that track events by user or by ScanStation to its web activity log and election activity log. An instance of the Tabulator application runs on each ScanStation computer, tracking the ballots scanned and printing to screen any errors encountered. These Tabulator messages are also written to the election activity log.

For each card image, the ClearCount software accurately tracks which ScanStation and scanner were used, as long as the documented procedure of confirming machine names and serial numbers is followed. This information is stored in the election database.

1.7.1.2 Accommodate device control functions

The ClearCount system accommodates all device-control functions, job duties, and responsibilities of central-count polling place officials and maintenance personnel. Any action that could affect vote count is controlled via technological means, administrative means, or both.

- Creating or deleting an election, setting the active election, changing the election phase, and backing up or restoring an election via the Election Administration pages are all password-protected and logged. Only a user with an access level of dbadmin or above can access and use these features.
- Creating or deleting users, assigning passwords, and assigning user permission levels in the User Administration pages are password-protected and logged. Only a user with an access level of useradmin (the highest level in the ClearCount system) can access and use these features.
- Vote modification using the Card Resolutions tool is password-protected and logged. Only users with an access level of modify or above can see and use this tool.
- Box deletion (prior to rescanning in the case of errors) is password-protected and logged. Only users with an access level of modify or above can see and use the DeleteBox utility.
- If any user attempts to scan a box a second time without the first being deleted, a Tabulator error is generated and logged.
- The ClearCount system automatically creates a set of election reports, which are described in detail in the *ClearCount Reporting Guide*. Access to these reports is password-protected and logged. Only users with an access level of read or above can see these reports. Access to reports that feature contest results prior to the close of polls is prohibited by statute.
- Opening the polls consists of starting up the hardware and beginning to scan.

- Closing the polls is controlled by a user with an access level of dbadmin or useradmin changing the election phase from Scanning to either Reviewing or Closed so no additional scanned cards can be accepted.

1.7.1.3 Register and accumulate votes

The Tabulator application registers and accumulates votes by boxes of scanned-in ballots. Each box is identified by a box ID, which itself forms part of the unique ID for the image for each side of the card.

1.7.1.4 Accommodate variations in ballot counting logic

The ClearCount system accommodates variations in ballot counting logic, including contest rotation and special handling for cross-party endorsements.

1.7.2 Voting variations

Responsive to VVSG 2005, Volume 1, Section 2.1.7.2.

Table 1-1 describes the ClearCount system support for specific voting variations.

Table 1-1. Voting variations

Voting variation	Description	Supported
Closed primaries	A primary in which only the registered members of a party can vote. Independent/Unaffiliated voters cannot participate. This variation is primarily implemented by the EMS.	Yes
Open primaries	A primary in which any registered voter can vote. This variation is primarily implemented by the EMS.	Yes
Primary presidential delegation nominations	Voters select their state’s delegates to their party’s national presidential nominating convention.	Yes
Split precincts	A precinct requiring more than one ballot because some of the contests are different. The ClearCount system treats these as separate precincts.	Yes

Table 1-1. Voting variations (continued)

Voting variation	Description	Supported
Write-in voting	<p>The ClearCount system reports the number of votes cast in each contest in write-in voting positions. If anything is written in the designated write-in area, it counts as a write-in vote. If a voter fills in an oval and a write-in, even for the same person, it counts as an overvote.</p> <p>The ClearCount system detects which write-in locations have writing by sampling the area of the write-in box.</p> <p>This is primarily a feature of the EMS. The ClearCount system supports the tabulation of the number of write-in votes. If anything is written in the write in area, it counts as a write-in vote.</p>	Yes (see note)
Cross-party endorsement	<p>Two or more parties endorse the same candidate and are listed separately on the ballot.</p> <p>If a voter votes twice for the same candidate (such as once as the Democratic candidate and once as the Working Families candidate), it is called a double vote. This does not disqualify the vote, but it only counts as one vote for that candidate. However, if the voter puts the same candidate in as a write-in vote and a regular vote, it counts as an overvote.</p>	Yes
Vote for N of M	<p>A multiple-winner voting system where voters select more than one candidate from a pool of candidates. For example, the ballot may instruct the voter to choose 3 of 5 candidates. Unlike cumulative voting, the voter cannot spend more than one vote on a given candidate.</p>	Yes
Nonpartisan offices	<p>An office for which a candidate cannot indicate a political party. Examples in some jurisdictions include judicial offices and school superintendent. The assumption is that these candidates should not take political positions into account when fulfilling their duties.</p> <p>There can also be a nonpartisan primary ballot for unenrolled voters, where they can only vote for nonpartisan offices.</p>	Yes

Table 1-1. Voting variations (continued)

Voting variation	Description	Supported
Partisan offices	<p>A public office for which a candidate can indicate a political party preference on his or her declaration of candidacy. That preference appears on the primary and general election ballot, along with the candidate's name.</p> <p>This variation is primarily implemented by the EMS.</p>	Yes
Ballot rotation	<p>The rotation of candidates' names to minimize the chance of order bias. For each ballot style, the ClearCount system identifies where the information is located and processes it accordingly.</p>	Yes
Straight-party or ticket voting	<p>The voter can mark a single oval to vote for all candidates of the specified party, without having to mark each individual contest's ovals.</p>	Yes
Provisional or challenged ballots	<p>Someone may show up to vote, but not be accepted due to lack of ID or some other confusion. Such a person can request a provisional ballot and then have a week to show up with proper ID.</p> <p>The ClearCount system does not have a mechanism to hold or outstack provisional ballots after they have been scanned. Instead, Clear Ballot advises jurisdictions to physically isolate and hold such ballots and not scan them until the underlying issues have been resolved.</p>	Handled procedurally (see note)
Recall issues, with options	<p>A recall or similar election where the voter votes whether to recall the official, and then votes for his or her replacement. If the recall fails, the second part is discarded. However, even if a voter votes against the recall, he or she can vote for a replacement candidate.</p>	No
Cumulative voting (also known as weighted voting or multivoting)	<p>A multiple-winner voting system where voters select one or more candidates from a pool of candidates. The voter has a number of votes and can spend them all on one candidate or divide them among candidates. The ballot design might feature columns of ovals next to candidate names.</p>	No
Ranked choice voting (also known as instant-runoff voting)	<p>Voters rank outcome in a hierarchy on the ordinal scale, expressing order of preference of the candidates. In an instant-runoff ballot, voters are instructed to rank any number of the candidates in numerical order.</p>	No

1.8 Ballot counter

Responsive to VVSG 2005, Volume 1, Section 2.1.8.

The ballot counter in the ClearCount central count system is called the Tabulator application. For information about the precinct ballot counter see the ClearCast documentation.

1.8.1 About the Tabulator application

In the ClearCount system, an instance of the Tabulator application runs on each ScanStation to analyze incoming image files from the scanner.

The Tabulator window appears on the ScanStation screen, where its status can be monitored. It conveys the following:

- Current status (page 45)
- Completion (page 45)
- Performance (page 45)
- Alerts (page 46)

Before and after scanning and tallying each box of ballots, the Tabulator application's status information displays zeroes in the Scanning, Adjudicating and Saving Images columns. With each ballot scanned, these numbers increment.

If an error occurs, such as a scanner misfeed or jam, an error message appears. A user with an access level of modify or above can delete the box, and the scanner operator can then rescan it.

The screenshot shows the 'Clear Ballot Status' window for 'xx_ClearCounty2015g'. The window title is 'Clear Ballot Status - xx_ClearCounty2015g - PaperStream IP fi-6400dj - AKHCC00252 - SCANSTATION06'. The interface is divided into several sections:

- Clear Ballot** (Logo)
- ELECTION**: xx_ClearCounty2015g
- SCANSTATION**: SCANSTATION06
- SCANNER**: Model: PaperStream IP fi-6400dj, Serial: AKHCC00252
- BOXES SCANNED**: (Empty list)
- CURRENT STATUS:** A table with columns: Scanning, Adjudicating, Saving Images.

	Scanning	Adjudicating	Saving Images
Current Box			
Total cards queued to be done	0	0	0
Time to completion	---	---	---
- COMPLETION:** A table with columns: Scanning, Adjudicating, Saving Images.

	Scanning	Adjudicating	Saving Images
Total boxes completed	0	0	0
Total cards completed	0	0	0
- PERFORMANCE:** A table with columns: Scanning, Adjudicating, Saving Images.

	Scanning	Adjudicating	Saving Images
Cards Per Minute	---	---	---
Cards Per Hour	---	---	---
Total unreadable cards		0	
Unreadable percentage		0.0%	
- ALERTS:**
 - 2016-10-13 04:18:42 Scanner PaperStream IP fi-6400dj serial AKHCC00252 connected
 - 2016-10-13 04:18:42 ClearCount (Version 1.3.2 2016-10-12) Tabulator Started

Figure 1-3. The Tabulator window

1.8.1.1 Tabulator window: Current status information

The Current Status section lets the scanner operator know where the Tabulator application is in its processing.

Table 1-2. Current status in Tabulator window

Item	Description
Current box	The unique identifier for the box being scanned, adjudicated, and saved. The box ID becomes part of the unique identifier for each card image in the box, which enables Clear Ballot's Ballot-to-Image Traceability feature.
Total cards queued to be done	The number of ballots in the queue for the scanning, adjudicating, and saving processes.
Time to completion	The time to completion for the scanning, adjudicating, and saving processes.

1.8.1.2 Tabulator window: Completion information

The Completion section tracks the status of the scanning operation.

Table 1-3. Completion information in Tabulator window

Item	Description
Total boxes completed	Number of boxes completed in this run of the Tabulator application. When the Tabulator application shuts down, the count is reset to 0.
Total cards completed	Number of cards completed in this run of the Tabulator application. When the Tabulator application shuts down, the count is reset to 0. This number includes cards with errors that did not successfully register.

1.8.1.3 Tabulator window: Performance information

The performance section tracks ballot-processing performance.

Table 1-4. Performance information in the Tabulator window

Item	Description
Cards per minute	Rate at which cards are being processed. This value is dynamic.

Table 1-4. Performance information in the Tabulator window (continued)

Item	Description
Cards per hour	Rate at which cards are being processed. This value is dynamic.
Total unreadable cards	<p>Number of cards or pages (including both sides) for which the Tabulator application failed to recognize and register the image as a ballot or target card. A value can only appear in the Adjudicating column.</p> <p>If there is an error on either side, the card is considered to have errors. The side without errors is successfully saved. When a user opens the erroneous card image in the Card Resolutions tool, the values for the side without errors are automatically filled in. The actual error message, which identifies where the error appears, is displayed on the Tabulator window and recorded to the election activity log.</p>
Unreadable percentage	Total unreadable cards divided by total cards completed. A value can only appear in the Adjudicating column.

1.8.1.4 Tabulator window: Alerts information

The Alerts pane appears at the bottom of the Tabulator window. The Alerts pane conveys status, warning, and error messages. After messages fill the visible area, users can scroll up and down to access the full set of messages.

The Tabulator Alerts pane displays the following types of messages:

- Information messages appear on a white background.
- Warning messages about errors that do not cause the Tabulator application to stop functioning appear on a yellow background. The information in these messages may still require a box to be deleted and rescanned. If a message appears repeatedly, report it to Clear Ballot Technical Support.

- Errors that appear with a red background cause the Tabulator application to stop functioning. To resolve such issues, a user with modify access level or above must delete the box using the DeleteBox utility as instructed in "Troubleshooting scanning issues" in the *ClearCount Election Administration Guide*, and then instruct the scanner operator to rescan that box. The DeleteBox utility deletes all saved images and election database entries from the box on the ScanStation and on the CountServer. Report the error to Clear Ballot Technical Support.

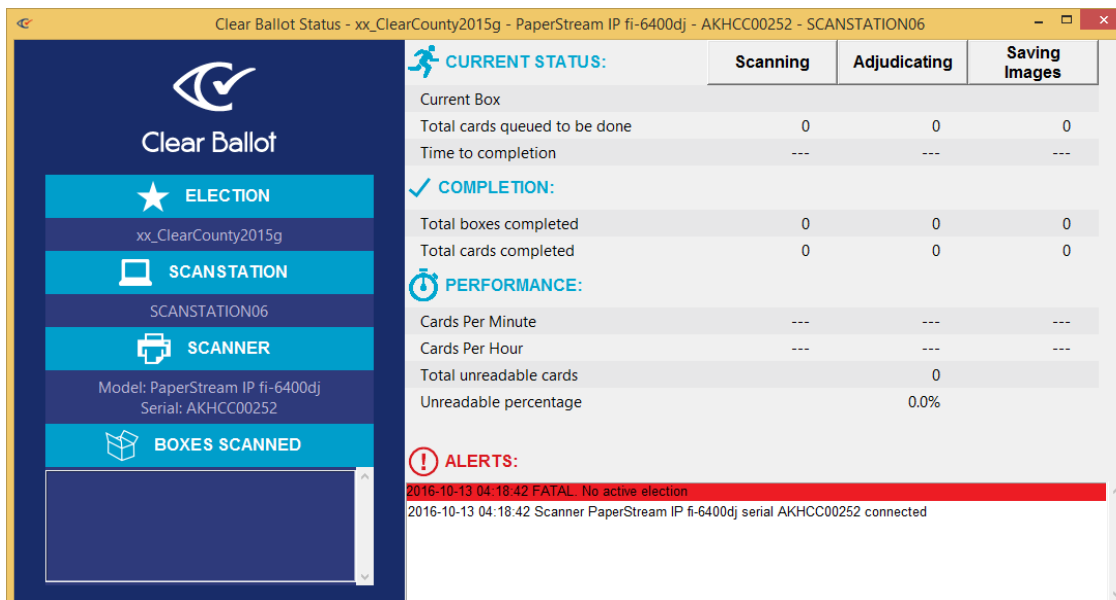


Figure 1-4. Example of a fatal Tabulator error

1.8.2 Ensuring the counter is set to zero

In the ClearCount system, after creating the election, but before scanning any ballots, you can create a zero report to prove that all vote totals are set to zero at the start of an election.

To produce the zero report:

1. Log in to a CountStation.
2. From the Election Index, select the election.
3. From the Dashboard, click the **Report** drop-down menu and select **Statement of Votes Cast**. The zero report appears.
4. Share the report as needed (copy, export to CSV, or print).

1.8.3 Resetting the counter

Resetting the counter on the Tabulator application occurs when it is restarted after shutdown. The CountServer maintains a database of the scanning statistics for each ScanStation. To reset the information for a box, a user with an access level of modify or above must enter a password to allow a specific batch to be deleted and rescanned.

1.8.4 ScanStation report

The ScanStation report summarizes the following information by ScanStation and Tabulator application:

- The number of boxes and cards scanned
- How many of those were unreadable, by number and by percentage
- When scanning started and stopped on that ScanStation, and the duration of scanning
- The rate of cards scanned by hour

1.9 Telecommunications

Responsive to VVSG 2005, Volume 1, Section 2.1.9.

The ClearCount system runs on a distributed, client/server model. However, it only communicates using a closed, wired Ethernet connection that prevents outsiders from gaining access. Each client ScanStation and CountStation is connected via Ethernet cable through a network switch to the CountServer. Wireless and public connections are not supported.

After ballots are scanned and tabulated, results from the election database are served as election reports accessible via browser from a CountStation. These reports can be accessed by any user with read access level or above.

1.10 Data retention

Responsive to VVSG 2005, Volume 1, Section 2.1.10.

The ClearCount central-count system works with jurisdictional election rules and personnel to safeguard ballots and retain data.

As part of its recommended workflow, the ClearCount system shares ballot chain of custody with the jurisdiction's election officials. The election officials select the site, hire staff, and set the level of site security required. The election officials or their delegates are on-site during the entire election process, ensuring ballot control before, during, and after the central-count scanning operation.

The ballots themselves serve as part of the audit trail. The ClearCount system does not physically mark or damage the ballots in any way during scanning. After scanning, ballots are reboxed and returned to the election officials, with the addition of target cards and box labels that make it easy to later find any physical ballot associated with a scanned image.

An additional layer of data retention comes from the ClearCount system itself, which includes the ability to back up an election (including its associated card image files). To comply with the 22-month retention requirement, a jurisdiction can choose to preserve the ClearCount election and associated images electronically. Alternatively, users can print a copy of the database, audit trail, and reports, and maintain the printed version for at least 22 months. The external hard drives, DVDs, and USB drives used for information retention are also suitable for retention periods of 22 months or more.

Chapter 2. Prevoting capabilities

Responsive to VVSG 2005, Volume 1, Section 2.2.

The following sections describe the prevoting capabilities of the ClearCount system.

2.1 Ballot preparation

Responsive to VVSG 2005, Volume 1, Section 2.2.1.

The ClearDesign EMS can import existing data created through other voting systems. See the ClearDesign product documentation for detailed information.

2.2 Election programming

Responsive to VVSG 2005, Volume 1, Section 2.2.2.

The ClearDesign EMS provides election programming capability. After the election is programmed, the ClearDesign EMS generates ballot style PDFs and the BDF needed by the ClearCount system.

For a description of the BDF, see the *ClearDesign Ballot Definition File Guide*.

2.3 Ballot and program installation and control

Responsive to VVSG 2005, Volume 1, Section 2.2.3.

The following sections describe the means of installing the ClearCount software on its central-count equipment.

2.3.1 Obtaining the ClearCount software

The ClearCount software is installed from a DVD. Jurisdictions obtain the software from Clear Ballot. The ClearCount product documentation is distributed on a disc that accompanies the installation DVD.

Jurisdictions can also obtain the software and documentation from Clear Ballot's voting system test laboratory, Pro V&V, as required, for EAC certification.

2.3.2 Detailed work plan

Steps and scheduling for software and ballot installation, including key dates, events, and deliverables, are indicated below:

Table 2-1. Example of election preparation and installation schedule

Date	Event	Related Deliverables
More than 45 days before the election	Election officials receive software from Clear Ballot for distribution to jurisdictions.	ClearCount software
More than 45 days before the election	Election officials install ClearCount software and verify that it is properly installed.	Expected hash code and version information
More than 45 days before the election	Election officials use the ClearDesign EMS to produce ballot style PDFs.	Ballot style PDFs for each precinct in the election
30 days before the election	Election officials use the ClearDesign EMS to generate an election definition, known as a ballot definition file (BDF).	Completed BDFs
30 to 15 days before the election	Election officials perform logic and accuracy (L&A) testing on the software and BDF.	L&A test results

2.3.3 Software verification

The ClearCount software is verified as part of readiness and L&A testing. As part of this testing, the jurisdiction should confirm that the correct election is installed and is selected as the active election. While scanning, scanner operators should monitor the Tabulator window on the ScanStation computer for any warning or error messages and inform the supervisor about such messages immediately.

For details, see "ClearCount logic and accuracy testing" in the *ClearCount Election Administration Guide*.

2.4 Readiness testing

Responsive to VVSG 2005, Volume 1, Section 2.2.4.

Clear Ballot has established policies and procedures to ensure readiness and allow election officials to feel confident about the stability and reliability of the system before launching the ClearCount central-count operation. Full details about ClearCount readiness testing can be found in the *ClearCount Election Administration Guide*.

2.5 Verification at the central location

Responsive to VVSG 2005, Volume 1, Section 2.2.6.

The ClearCount central-count system does not include a polling-place component. It provides a formal record of the following items in the manner described below:

- Before scanning the ballots, a unique entry in the election database is created for each election. All data for that election is stored under that name.
- Each ScanStation is identified by a name that appears on the physical unit and in any references to it in the Tabulator application and other applications. Before scanning, operators are instructed to confirm that the ScanStation name, the election name, the scanner model, and the computer serial number appear correctly on the Tabulator window.
- The test deck should include all used ballot formats.
- Following election creation, but before any cards are scanned, the jurisdiction must check the Statement of Votes Cast report to ensure that all vote and ballot counts are set to zero. As needed, the jurisdiction can print or export this report.

The ClearCount readiness testing confirms that there are no hardware or software failures, and that the devices are ready to be activated for accepting votes.

2.5.1 Verifying installation and interfaces

The ClearCount installation can be verified by confirming the versions of each component. Log into ClearCount via a CountStation, click the login drop-down menu and select **About this Software**.

The ClearCount About this Software page contains two tabs. Clear Ballot Product Files tab lists filenames, dates, and file digest information about ClearCount system files. The Installed System Packages tab lists filenames, dates, and file digest information for third-party packages used in the ClearCount system.

The *ClearCount System Identification Guide* lists every system file and package.

2.5.2 Verifying the hardware functionality

The ClearCount system consists of the following hardware components, each of which can be verified separately and in combination:

- One CountServer
- One or more ScanStations with an attached scanner
- One or more CountStations
- The local area network (LAN) hardware consists of the network switch and Ethernet cables

2.5.2.1 Verifying the CountServer

The CountServer software runs on a COTS computer. To verify that the computer hosting the CountServer is functioning properly, start it up as documented by the manufacturer.

2.5.2.2 Verifying the CountStations

Each CountStation consists of a COTS computer with a browser installed. This computer is part of the ClearCount closed, wired network.

To verify the operation of a CountStation, connect it to the ClearCount network and log in as documented in the *ClearCount Election Administration Guide*.

2.5.2.3 Verifying ScanStations

Each ScanStation is a COTS computer that is attached to a scanner via a USB cable. This computer is part of the ClearCount closed, wired network.

To verify the operation of a ScanStation, connect and run the computer and the scanner as documented in the *ClearCount Election Administration Guide*.

2.5.2.4 Verifying the LAN hardware

The ClearCount system is a distributed system that requires a wired Ethernet connection. To verify the operation of the network switch, start it as documented by the manufacturer.

2.5.2.5 Verifying the full ClearCount system hardware

To verify a full ClearCount system, set up a full system, consisting of:

- A CountServer
- At a minimum, one ScanStation with an attached scanner
- At a minimum, CountStation
- A network switch, along with the necessary Ethernet cables

Install and configure the system as documented in the *ClearCount Installation Guide*.

2.5.3 Verifying the software

The ClearCount software components can be verified as documented in the *ClearCount System Identification Guide*.

2.5.4 Generating consolidated data reports

The ClearCount system consolidates the ballot data collected from each ScanStation into an election database that resides on the CountServer. The CountServer serves a set of browser-based election reports for each election. These reports are accessible on a CountStation via the Dashboard, which provides an overview of the current state of the election scanning process, as well as links to a number of specialized reports.

2.5.5 Segregating test data from actual voting data

Readiness and L&A testing of the ClearCount system are done using a test version of the election. This test should use the same test ballots that were used with the state-certified EMS. After generating the necessary proofs and reports from the test database, election officials back up the test election and then delete the results of the test from the active system.

2.5.6 Test simulation software

The ClearCount system does not include any test simulation software.

2.5.7 Testing all ballot positions

A jurisdiction's readiness test must test all ballot positions. The jurisdiction should mark a test deck to a known result in accordance with its testing procedures. The jurisdiction should scan the test deck and compare the results of the ClearCount Statement of Votes Cast report with the expected results.

For details about readiness testing, see the *ClearCount Election Administration Guide*.

2.5.8 Verifying equipment readiness

Clear Ballot has established policies and procedures to ensure readiness so that election officials feel confident about the stability and reliability of the system before launching the ClearCount central-count operation.

For details about readiness testing, see the *ClearCount Election Administration Guide*.

2.5.9 Obtaining status and data reports

An election database allows ClearCount system users to obtain status and data reports from individual ScanStations, as well as the system as a whole.

2.5.9.1 Obtaining reports about individual ScanStations

The Tabulator application allows the CountServer to analyze local documents and transfer them to the CountServer output folder. One instance of the Tabulator application runs on each ScanStation. Each instance of the Tabulator application logs actions as they occur. These actions are also logged to the election activity log, as described in "Event recording, logging, and tracking" on page 34.

The ScanStation report provides information about the activity time and number of cards processed by the Tabulator on each ScanStation. ScanStations are identified by name in the first column. The *ClearCount Reporting Guide* describes the report.

2.5.9.2 Obtaining reports from the election database

The election database holds the consolidated election results and serves them in the form of election reports that election officials can use to track, analyze, and disseminate election results.

Chapter 3. Voting capabilities

Responsive to VVSG 2005, Volume 1, Section 2.3.1.

Because the ClearCount system is a central-count system only, opening the polls for voting consists of starting up the hardware and beginning to scan.

3.1 Verifying ballot-marking devices

With the ClearCount system, ballot-marking devices are verified during pre-election testing. Verification ensures the scanners are properly reading acceptable ballot-marking devices. For more information about ballot-marking devices, see "Paper-based recording requirements" in the *ClearCount Hardware Specification*.

3.2 Voting booth facility

The ClearCount system does not address this requirement because precinct voting is covered by the ClearCast precinct system.

3.3 Secure receptacles for holding voted ballots

Voted ballots are packaged and transferred to the central-count location by the jurisdiction in receptacles of the jurisdiction's choice. Following the ClearCount central-count scanning operation, the ballots are returned to these receptacles.

An identifying ClearCount box label (2 x 4 inches) is added to the outside of the receptacle, but the receptacle is not otherwise modified by the process.

3.4 Activating a ballot-counting device

In the ClearCount system, activating the ballot-counting device takes place when the scanner operator scans the first batch of ballots, starting with its target card. As cards are scanned on a ScanStation, the Tabulator instance counts and records the votes.

3.5 Verifying the device

Verifying that the ballot-counting devices have been correctly activated is part of readiness testing (documented in the *ClearCount Election Administration Guide*). Verifying that the ballot-counting devices are functioning properly consists of monitoring the Tabulator window on the ScanStation computers, as well as monitoring the election activity log.

3.6 Casting a ballot

Responsive to VVSG 2005, Volume 1, Section 2.1.8.

Because the ClearCount system is a central-count system, voters do not interact directly with it. Scanner operators scan the accumulated voted ballots at a central-count location.

3.7 Identifying device failure and associated corrective action

For information about identifying and correcting device failure, see the *ClearCount Maintenance Guide*.

Chapter 4. Postvoting capabilities

Responsive to VVSG 2005, Volume 1, Section 2.4.

This chapter describes the postvoting capabilities of the ClearCount system.

4.1 Closing the polls

Responsive to VVSG 2005, Volume 1, Section 2.4.1.

Because the ClearCount system is a central-count system, *closing the polls* means registering a log entry that indicates that ballot processing is complete, and preventing the system from processing additional ballots without an explicit, loggable command to do so. This consists of a user with the access level of dbadmin or useradmin changing the election phase from the Scanning phase to either the Reviewing or the Closed phase so that no additional scanned ballots can be accepted. The action of changing the election phase is logged in the election activity log.

Similarly, *reopening the polls* in the ClearCount system requires a user with the access level of dbadmin or useradmin to change the election phase back to Scanning. The action of changing the election phase back is also logged in the election activity log.

In general, a jurisdiction closes an election when its administrators are satisfied that all ballots are scanned, tabulated, and resolved. Some election administrators compare their ballot numbers to the numbers recorded by the precinct (garnered through poll books or another recordkeeping mechanism), while others keep track of the number of boxes of ballots. Because precinct-level tracking is not always exact or scientific, a small discrepancy of a few ballots is sometimes acceptable. Users can determine that they are not missing any precincts or ballot boxes by ensuring that all precinct and box IDs are represented in the ClearCount system.

4.1.1 Shutting down the ClearCount system

In the ClearCount system, a distinction is made between shutting down the system for the day (with the intention of resuming ballot processing at a later date), and closing the polls (that is, completing election processing to the best of the election officials' knowledge).

4.1.1.1 Resolving unreadable cards

The ClearCount Card Resolutions tool is used to resolve unreadable cards. Updates related to unreadable card resolution automatically modify the election when the user has the correct level of access and the election is in the appropriate phase. Resolving cards must occur at the central-count location on a CountStation.

There are two classes of unreadable cards—those with physical issues, which are generally not controversial, and those with voter intent issues, which require judgment to resolve.

Examples of physical issues include a folded card or one with a Post-it note stuck to it. After election administrators address the physical issue, they can rescan the card or manually review it, depending upon the guidelines set by the jurisdiction. If a large number of physical issues arise, jurisdictions are advised to consult with Clear Ballot Technical Support.

For Card Resolutions tool procedures, see "Examining and processing unreadable cards" in the *ClearCount Election Administration Guide*.

After processing all unreadable cards, the election official should state that the election is closed. That statement and the accompanying action are logged. After that, a specific, logged action performed by a user with administrator credentials is required to reopen the election to additional changes. This might be necessary if previously unscanned cards are discovered, or if provisional ballots need to be considered later.

4.1.1.2 Viewing reports for a closed election

Requirements for viewing the ClearCount election reports include the following:

- The CountServer must be running. It can operate on a computer in a nearby secured room if it can be Ethernet-wired to the network switch connected to the CountStations.
- Election officials must have a wired connection to the CountServer. (This means election officials must be present at the central-count facility to monitor results on a CountStation.)

Data is shared by exporting results to CSV or text files. To back up an election, a user with dbadmin access or above saves a read-only copy of the database to an external hard drive. The files can be restored to a ClearCount system running the same version of ClearCount software.

4.1.2 Shutting down with a planned restart

The ClearCount system is designed so that jurisdictions can begin scanning and adjudicating ballots in advance of Election Day. The ClearCount system can process ballots over the course of several days. This is essential if a jurisdiction permits mail-in or absentee ballots.

In larger jurisdictions, it may take more than one day to complete scanning even when processing only Election Day results. To accommodate multisession scanning, the ClearCount system can be shut down and restarted between boxes, with result tabulation picking up where it left off.

For shutdown instructions for the ClearCount system, see "Interrupting and resuming scanning" in the *ClearCount Election Administration Guide*.

Chapter 5. Consolidating vote data

Responsive to VVSG 2005, Volume 1, Section 2.4.2.

This chapter describes how vote data consolidation functions with the ClearCount system.

5.1 How ClearCount consolidates voting data

The ClearCount software follows a distributed computing model to foster both speed and scalability. Setup consists of a LAN with one or more ScanStations and one or more CountStations connected to a single CountServer.

No ClearCount software is installed on a ScanStation or CountStation computer—only the scanner drivers and software. Each ScanStation and CountStations, used for ResultsUploader, has a remote network drive mapped to the CountServer, from which it accesses the image-processing and analysis software.

The CountServer runs the Ubuntu Linux operating system and comprises:

- A minimal read-only file server suitable for gaining centralized access.
- A relational database server. The adjudication goes here.
- A web server, used for accepting upload requests of images. This allows officials to view election results, including voted ballots that require manual review.

The ClearCount system consolidates the results from the each ScanStation and ClearCast unit into a single election in the election database. These results, in the form of election reports, can be exported in CSV or text format.

5.1.1 Consolidating data from ScanStations

The scanner sends each image to the ScanStation's hard drive, which analyzes and adjudicates the ballots. ScanStation computers send the data to the CountServer; they do not retain it.

5.1.2 Consolidating data from ClearCast

The ResultsUploader application, running on a CountStations, is used to transfer the ClearCast voting data to the CountServer for consolidation of the voting data. The ResultsUploader monitors for the insertion of a USB stick that has valid ClearCast data and then transfers that data to the CountServer using the HTTPS protocol. The ClearCount server then consolidates those results into the active election.

5.2 Producing reports

Responsive to VVSG 2005, Volume 1, Section 2.4.3.

The ClearCount system generates a series of reports that election officials can use to review and analyze vote data and election results. These reports can be accessed via a browser on a CountStation, which is connected to the CountServer using a closed, wired Ethernet connection. (While the data used to create the reports is read-only, the user can filter results and resize images in many of the reports.) The reports can also be exported in CSV or text file format, as well as printed.

Jurisdictions can prevent production of results reports before it is legal to produce results by turning off the Display Vote Totals option on the Election Administration page for an election.

A summary of all of the report types the ClearCount system creates can be found in the *ClearCount Reporting Guide*.

The ClearCount system supports geographic reporting to the level required. The level of geographic granularity at which the ClearCount system reports reflects the level supported in the election.

- The ScanStation report summarizes the performance of each scanner and its associated Tabulator instance, including the number of cards processed by this unit.
- The Statement of Votes Cast report provides the results of each contest, by vote, overvote, undervote, and nonvote. For each selection, the election official can access precinct, counter group, and party subtotals.
- The Statement of Votes Cast report provides the results for each contest of all votes cast.

The ClearCount system produces two logs, the web activity log and the election activity log, both of which can be printed or exported. For details, see "Event recording, logging, and tracking" on page 34.

The ClearCount reports are served by a web server that resides on the CountServer. The web server does not modify the source data of an election in any way. While report readers can access data in the reports, they cannot send a request to modify the election back to the web server.

The reports generated by the ClearCount system are password-protected to prevent unauthorized access. In addition, some jurisdictions enforce procedural controls over access to certain reports. For example, election officials can consult certain election reports before the close of polls to see how many precincts have been processed, but they cannot access cumulative results data reports, such as those that appear in the Statement of Votes Cast report.

5.2.1 Geographic reporting

The ClearCount system supports geographic reporting, including split precincts. The level of geographic granularity at which the ClearCount system reports reflects the level supported in the election.

5.2.2 ScanStation reports

The ScanStation report summarizes the performance of each scanner and its associated Tabulator instance, including the number of cards tabulated by this unit.

The Statement of Votes Cast report provides the results of each contest by vote, overvote, undervote, and nonvote. For each selection, the election official can access precinct, counter group, and party subtotals.

5.2.3 Consolidated printed reports

The Statement of Votes Cast report provides the results for each contest of all votes cast.

5.2.4 Printed reports based on user queries

The ClearCount system allows election officials to export individual reports from a CountStation as text or CSV files to a USB drive. They can then be copied to a computer and printed.

5.2.5 System audit reports

The ClearCount election activity log and web activity log can be exported from a CountStation as text or CSV files to a USB drive. They can then be copied to a computer and printed.

For details, see "Event recording, logging, and tracking" on page 34.

5.2.6 Data protection in the reporting process

The ClearCount reports are served by a web server that resides on the CountServer. The web server does not modify the source data of an election in any way. While users can access and filter or resize the data returned in the reports, they cannot send a request to modify the election back to the web server.

The reports generated by the ClearCount system are password-protected to prevent unauthorized access. Further, generation of results-oriented reports is statutorily controlled to prevent information that might influence outcomes from being released prematurely. Election officials can consult other reports during the election to see, for example, how many precincts have been processed, but they cannot access cumulative results data reports, such as the Statement of Votes Cast report.

For more information, see "Protection of data input and storage" on page 28

5.2.7 Exporting report data

The ClearCount system allows election officials to export individual reports from a CountStation as text or CSV files to a USB drive.

5.2.8 Consolidating polling-place data into a single report

Because the ClearCount system is not a polling-place system, this document does not address the requirement to consolidate the data contained in each unit into a single report for the polling place.

5.2.9 Data and report protection

The ClearCount system design does not allow report generation or transmission of results to alter the base election memory (other than generation of relevant entry into a log file).

5.2.10 Summary of reports created by the ClearCount system

For a description of the reports created by the ClearCount system, see the *ClearCount Reporting Guide*.

5.3 Broadcasting results

Responsive to VVSG 2005, Volume 1, Section 2.4.4.

The ClearCount system does not offer the capability to make unofficial results available to external organizations.

Chapter 6. Maintenance, transportation, and storage

Responsive to VVSG 2005, Volume 1, Section 2.5.

This chapter summarizes the maintenance, transportation, and storage requirements for the ClearCount system. For detailed information, see the *ClearCount Maintenance Guide*.

Because the ClearCount system is built upon unmodified COTS hardware, users are also referred to the manufacturer documentation included in the TDP.

6.1 Performing routine maintenance

As part of normal use, scanners need to be cleaned on a regular basis.

6.1.1 Cleaning schedule

During scanning operations, Clear Ballot recommends that the scanners be cleaned every 10,000 pages, or approximately once every 4 hours. The recommended workflow is documented in the *ClearCount Maintenance Guide*.

6.1.2 Cleaning instructions

For detailed instructions on how to clean each model of scanner, consult the manufacturer's documentation (included with the TDP).

6.1.3 Cleaning materials

The scanner manufacturers sell cleaning materials specifically designed for use with their scanners. For details about the materials needed to clean scanners properly, see the manufacturer's documentation.

6.2 Replacing scanner consumables

Scanners contain parts that need to be replaced on a regular basis. These parts are called consumables, and include:

- Pick rollers
- Separator rollers
- Brake rollers
- Pad assemblies

For large scanning operations, jurisdictions are advised to start with fresh rollers to minimize the possibility of having to replace them in the middle of the operation. For more information about obtaining and installing replacement rollers, see the manufacturer's documentation for the applicable model of scanner.

6.3 Performing specialized maintenance

Clear Ballot strongly encourages every customer to enter into a service contract with the scanner manufacturers. Scanner service technicians are able to diagnose, service, and, if necessary, replace a malfunctioning scanner quickly.

For full details of ClearCount maintenance, see the *ClearCount Maintenance Guide*.

6.4 Transportation and storage

Clear Ballot recommends that jurisdictions transport and store the hardware used in the ClearCount operation in its original boxes or in custom storage cases. The largest and heaviest component in the ClearCount system is typically the scanner, which can weigh up to ~70 pounds.

Between elections, jurisdictions are expected to store ClearCount hardware in a secure, climate-controlled location. No equipment used for voting should be repurposed for alternate use. Jurisdictions should consult the manufacturer's documentation for their COTS hardware to obtain specific guidance. At a minimum, the following conditions for storage are required:

- 15° to 35° C
- 20–80% humidity

Appendix A. Evaluating marks on paper ballots

Considerations include:

- Vote targets
- Ballot layout
- Ballot processing by the scanner vendor hardware and software
- Ballot processing by the Tabulator application (Clear Ballot software)
- Additional information about ballot mark recognition

A.1 Vote targets

A ballot contains a number of sensitive areas, referred to as *vote targets*, into which a voter enters marks to cast a vote. Depending upon the EMS vendor creating the ballot, the targets may appear as ovals, rectangles, or as a blank area between a set of right- and left-facing arrows that the voter must connect with a line.

Each target is associated with a choice name, such as a candidate name or a yes or no answer to a referendum question, or a choice name label containing the phrase *write-in*.

The targets and their choice names are grouped into named contests. A single side of a single ballot card may contain one or more contests.

This section describes the algorithms and strategy used by the ClearCount software to determine where the vote targets are located on the ballot and whether or not the target has been sufficiently marked to be considered a vote. After a card has been analyzed, each vote target is classified based on how it and other targets in the same contest have been marked. The classification categories are:

- **Voted**—The target is marked and no other targets in its contest are classified as overvoted.
- **Overvoted**—The target is marked, but more targets in its contest are marked than allowed by the contest's *vote rule*. The vote rule is the number of choices that can be marked for a contest.
- **Undervoted**—The target is not marked, and not enough targets in its contest are classified as voted to reach the maximum allowed under the contest's vote rule.
- **Not voted**—The target is not marked, but at least one other target in its contest is classified as voted or overvoted.

This section describes how vote targets are found and how marks on them are analyzed and interpreted. It does not describe how the results of those interpretations are recorded. For this information, see "Recording and tabulating cards" in the ClearCount Software Design and Specification.

A.2 Ballot layout

The layout of an unmarked ballot describing its contests and choices is represented in the following ways:

- **In a page included in a set of PDF files provided by the election officials.** Each PDF file contains one or more pages, and each page describes a single side of a ballot card. The PDF file may contain more than two pages, since an election typically consists of multiple ballot styles (multiple cards per ballot, multiple precincts per election each with their own ballots, and so on). The pages describe such things as the contest positions (physical locations on the ballot), and their associated choice names and vote target positions. The pages also contain a set of vendor-specific markings (known as the *code channel*) used to convey such items as an election-wide identifier for each ballot card (the *ballot-style-identifier*) and, very often, a precinct identifier. When setting up an election, the ClearVote software processes the PDFs to create the BDFs.
- **In a set of ballot definition files (BDFs) using standard comma-separated values format.** These files are produced when setting up the election, before any voting is done, by analyzing the PDF files using ClearVote software tools. The files describe such things as the ballot style, the precinct, each contest name and the associated choice names and the coordinates of the corresponding vote targets. When setting up an election, the ClearCount software processes the BDFs to create and initialize a MySQL database on the CountServer.
- **A single MySQL database is set up on the ClearCount CountServer once per election.** When a ClearCount ScanStation starts up, it uses MySQL transactions to retrieve the ballot layout information. The ScanStation uses additional MySQL transactions to this same database to record the results of an adjudicated ballot.

A.3 Ballot processing by the scanner vendor hardware and software

A.3.1 Scanner vendor hardware

A computer, attached using a USB cable, is used to drive a COTS scanner that has four functions:

- Feed ballot card stock quickly and efficiently
- Capture the front and back card images at a prespecified quality level and format
- Detect multifeeds
- Pass the images to COTS scanner software that runs on the computer

Depending upon the size and budget of the election jurisdiction, different hardware may be sourced. However, the basic software capabilities for each hardware model are the same.

A.3.2 Scanner vendor software

Ballot counts and vote totals are typically reported by precinct and counter group. While the precinct identifier is typically encoded into the ballot's code channel, the counter group relies on physical segregation of cards. To enable counter group-level reporting, cards must be segregated by counter group. To maintain cards control, scanning is performed one box (batch) at a time. The use of a target card and corresponding box label allows both requirements to be met.

During the scan, the scanner vendor's software performs the following sequential functions:

1. **Identifies the batch**—A *target card* is the first card scanned. It contains a barcode that identifies both the counter group and a box ID. The value of the barcode is used to associate each pair of card image names with a label affixed to the ballot storage box. For example, a target card with the barcode AB-001 indicates absentee ballots contained in a box with a label showing AB-001.
2. **Captures the card images**—By default, card images are formatted as industry-standard JPEG images and captured at 200 dpi (dots per inch), 8-bit grayscale.
3. **Names the images**—The scanner software uses the value of the barcode on the target card and an image sequence number to name card images uniquely. Odd sequence numbers are assigned to the first side, even numbers to the second side. For example, the card ID AB-001+10035 points to the thirty-fifth image from the target card (image AB-001+10001) for the absentee (AB) counter group and box 001. Card ID AB-001+10036 is assigned to the second side of the card as it goes through the scanner.
4. **Prepares the card image**—The scanner hardware and software then checks that only one card is being processed, captures both sides as two card images, deskews both card images, and crops the images to the physical size of the card.
5. **Saves the card images**—The scanner software saves each pair of card images in a JPEG format into a prespecified folder which is then processed by the Tabulator application.

In this way, processing cards can be done by any scanner software capable of reading a barcode, using the barcode and a generated sequence number to name an image, deskewing the image, cropping it, and saving it as a high-quality JPEG file in a prespecified folder. Most commercial scanner hardware vendors can provide software with this functionality.

A.4 Ballot processing by the Tabulator application

The Tabulator application is software that processes card images to count the votes for every candidate/choice. An instance of the Tabulator application runs on each ScanStation computer and analyzes each pair of card images in the following sequence:

A.4.1 Image grouping

Because the scanner vendor's image capture software places card images in a folder, the Tabulator application can run asynchronously with the scanner. In some instances, it may be necessary that the scanner be used simply to capture images for later processing instead of processing the card images in real time. In either situation, the Tabulator application looks for the next two consecutively named JPEG files to show up in a prespecified folder on the local hard drive. These two files are the images for the front and back of the next unprocessed ballot card.

A.4.2 Image registration

Registration is the process of determining the logical front of the ballot card and its readable orientation, and then locating all important *landmarks* on the image (for example, *timing marks* and the marks in the code channel). Ballots can be fed into the scanner in any order (such as back first), any rotation (for example, upside down) and any orientation (landscape or portrait). The Tabulator application registers each JPEG image by looking for known landmarks, the size and location of which vary by voting system vendor. As each ballot is scanned:

1. The Tabulator application determines how to find the landmarks by knowing the type of ballot, which is contained in a field in the metadata file, which is included with the set of BDFs defining the election. By analyzing the landmarks, the Tabulator application determines which physical side corresponds to the ballot's front.
2. Edge marks are used to precisely determine the amount of image skew and to correct for slight distortions in the ballot caused by the scanner. These edge marks form an imaginary grid where the intersections of horizontal and vertical lines are the only valid positions for the center of a vote target.
3. When the type of ballot does not have any edge marks (such as Hart, Sequoia), the Tabulator application looks for specific landmarks on the image and uses them to form the imaginary grid used to locate vote targets.

If, for any reason, one or both images fail registration, a record is written to the election database indicating the date, the time, and the failure code. Ballots that fail registration must go through digital ballot duplication using manual adjudication for their results to be included in the totals. See "Registration failure messages" in the *ClearCount Election Administration Guide* for more information.

A.4.3 Card identification

The code channel is decoded by the Tabulator application to determine the card style ID that is used to determine the layout of vote targets on the ballot. When the ballot-style-identifier is known, all relevant BDF entries can be found so the ballot can be analyzed for the location of the vote targets and their association with candidate/choice names that, in turn, are assigned to contests. Precinct assignment is also made based on IDs in the code channel, if present.

A.4.4 Mark analysis

The goal of mark analysis is to classify a vote target in such a way that an unbiased human observer would agree that regardless of the vote rule:

- No vote targets that are clearly empty are declared a vote (false positive).
- No vote targets that have an obvious mark are declared a nonvote (false negative).

In an ideal world, jurisdictions would use uniform white ballot stock, ballot printing companies would print ballots uniformly, image scanners would interpret the same mark the same way, and voters would completely fill vote targets. In that world, the job of discriminating between marked and unmarked vote targets is easy. But in the actual world, this is seldom the case for variety of reasons, including the following:

- Some jurisdictions use colored card stock to distinguish certain ballots. In addition, manufacturing techniques can result in ballots that are not uniformly colored.
- There may be differences in the printers used to print ballots. This is especially true where ballots printed on ballot-on-demand printers result in different grayscale values for the outlines of a vote target.
- There are two cameras in each scanner—one for each side of the ballot. Toner or paper dust buildup on either camera lens can lead to contrast and lightness inconsistencies, including differences that accumulate over time by the mere act of scanning.
- Ballots, especially vote-by-mail and absentee ballots, can be folded, leading some voting systems to detect marks where none exist.
- Voters have different marking styles, and so vote targets are not always marked in the same way from one voter to the next, or even for the same voter from one contest to the next.
- A voter can leave stray unintended (*hesitation*) marks within a vote target.
- A ballot could be stained or smudged.

Clear Ballot has developed a set of routines, outlined below, that, given properly printed ballots and properly maintained scanners, reasonably meets these goals.

A.4.4.1 Discriminant function

In statistics, a discriminant function is a mathematical or algorithmic *knife* that divides a population into two groups. To account for the inherent variability in the scanning process, and the inconsistency of human marking technique, Clear Ballot has developed a set of discriminant functions that successively divides the population of vote targets on a paper ballot into two groups—potential votes and not-votes. Potential votes become votes when they satisfy the vote rule and successfully pass through each of the three discriminant functions.

A.4.4.2 Noise floor concept

To implement the discriminant function, a concept from signal theory is employed—the *noise floor*. In signal theory, the noise floor is the measure of the signal created from the sum of all the noise sources and unwanted signals within a measurement system, where noise is defined as any signal other than the one being monitored. Applied to the classification of vote targets, the signal being monitored is the expression of voter intent. The unwanted signals are described in the bullets above.

The vote target scores and the noise floor are computed as follows:

- **Vote target scores**—Each vote target on the ballot, located through the image registration process (described previously), is assigned a score from 0 to 100, indicating its level of darkness. High scores are assumed to reflect affirmative voter intent. The vote target score is derived by analyzing the grayscale value of every pixel contained in the shape of the vote target. Therefore, a vote target with every pixel marked by a #3 pencil has a lower score than a vote target filled with a black felt-tipped marker. The scoring algorithm sums the darkness values of each pixel in the target, and then normalizes that total relative to what the score would be for a target that is 100% black.
- **Noise floor calculation**—The noise floor is computed as the lowest score of an empty vote target on each ballot side. Each ballot has two noise floors, one from each side of the ballot, which capture variations in the lighting conditions between the two cameras inside the scanner, as well as variations in paper stock (for example, colored ballots).

After the noise floor has been computed for both sides of the ballot, three discriminant functions are successively applied to divide the population of vote targets into two groups—potential votes and not-votes.

The basic strategy is first to divide the population so the number of visually empty vote targets is as few as possible in the potential votes group. Then, with two additional discriminant functions, the potential votes group is further winnowed, leaving vote targets that can then be submitted for vote target classification (described below).

- The first discriminant function (DF1) initially overclassifies vote targets (a potential vote target may later be reclassified as a not-vote). In this step, the determination is made based on whether each mark is sufficiently above the noise floor.
- The second discriminant function (DF2) further divides the population of potential votes from DF1 into the same two groups—potential votes and not-votes. The vote targets in each contest are compared to one another to determine which may represent stray marks. These appear as scores sufficiently different from other, more definite, potential votes in the same contest.
- The final discriminant function (DF3) further divides the potential votes into the same two groups. The vote targets across the ballot are compared to other targets classified as potential votes to determine which may represent stray marks. These appear as scores sufficiently different from other potential votes across the ballot.

The algorithms used by the three discriminant functions and the thresholds relative to the noise floor used to reclassify potential votes as not-votes have been predetermined after extensive experimentation with hundreds of thousands of actual voter-marked ballots. This algorithm can only be modified by Clear Ballot.

A.4.5 Vote target classification

For each contest, vote target classification applies the voting rule (such as, *Vote for 1* or *Vote for Not More than 3*) and state law to determine which potential vote targets have been classified as votes or overvotes, and which "not-vote" targets are classified as undervotes or nonvotes. See "Vote target classification diagram" on the next page.

Special cases:

- *Write-in votes*—At least one certified voting system does not use an oval as a vote target for write-ins. In this case, the *sensitive area* is considered to be the bounding box surrounding the write-in zone, and any mark is automatically determined to be a potential vote and is also classified as a vote or overvote depending upon the vote rule.

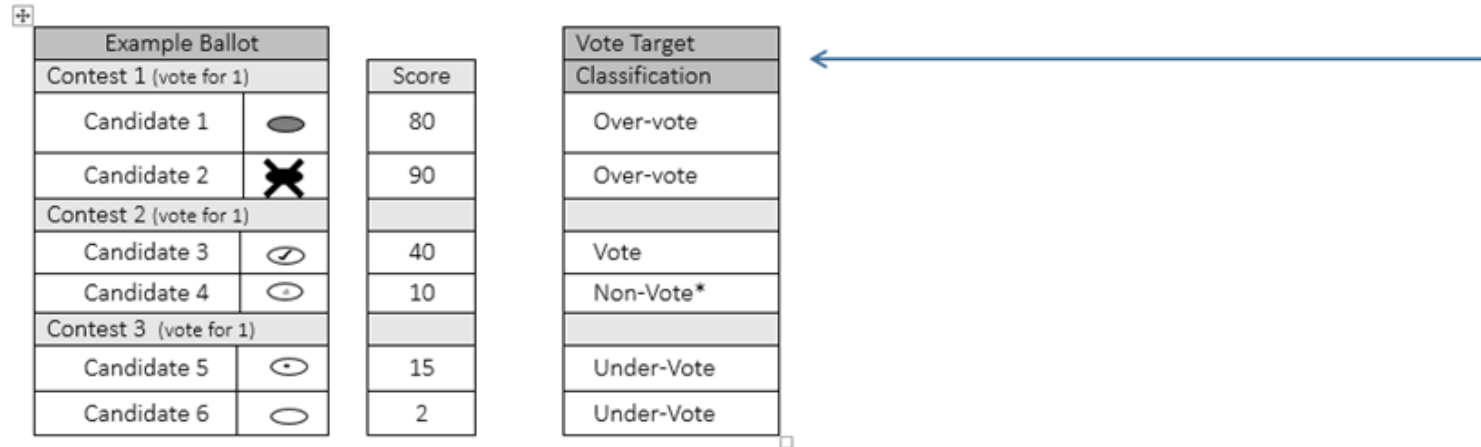
A.4.6 Result storage

After a ballot is processed, the Tabulator application sends the results of the analysis to the database server. These results include the classification of every vote target and the *provenance of the ballot*. The provenance records everything known about that ballot, including the date and time of the scan, the ScanStation ID, the scanner model, the serial number of the scanner, the card ID, the image filename, the precinct ID, and the card style ID. When human judgment is applied to the classification of votes, the user name, date and time are also recorded.

After the database server has confirmed the transaction, the Tabulator application copies the two card image files to the CountServer and, upon confirmation, deletes them from the ScanStation.

A.4.7 Vote target classification diagram

Example Ballot, Application of the Discriminate Function and Vote Target Classification



Application of the Discriminate Functions (DF) and Classification of the Vote Targets

Classified as		DF1	DF2	DF3	Vote Target Classification	
		Initial classification of marks on the same ballot	Marks compared to other marks in the same contest	Mark compared to other marks on the same ballot	Classifies every vote target into four distinct categories according to the voting rule and state law	
Potential Vote		 Representative scores			Votes	
Not-a-vote		 Noise floor			Over-Votes	
					Under-Votes	
					Non-Votes*	
Comment	All vote targets initially classified as not-votes	Coarse classification tries to classify vote targets so that all targets with marks are grouped as "potential votes".	Reclassifies marks with sufficiently different scores than other marks in the same contest	Further reclassifies marks inconsistent with sufficiently voted marks elsewhere on the ballot	* Non-votes are vote targets that have been grouped as "not-a-vote" in contests where the vote rule has been satisfied.	

Figure A-1. Vote target classification

A.4.8 Sample ballots

In the following two sample ballots, landmarks are identified with red circled areas and code channels with shaded areas:



Figure A-2. ES&S (ElectionWare election management system)

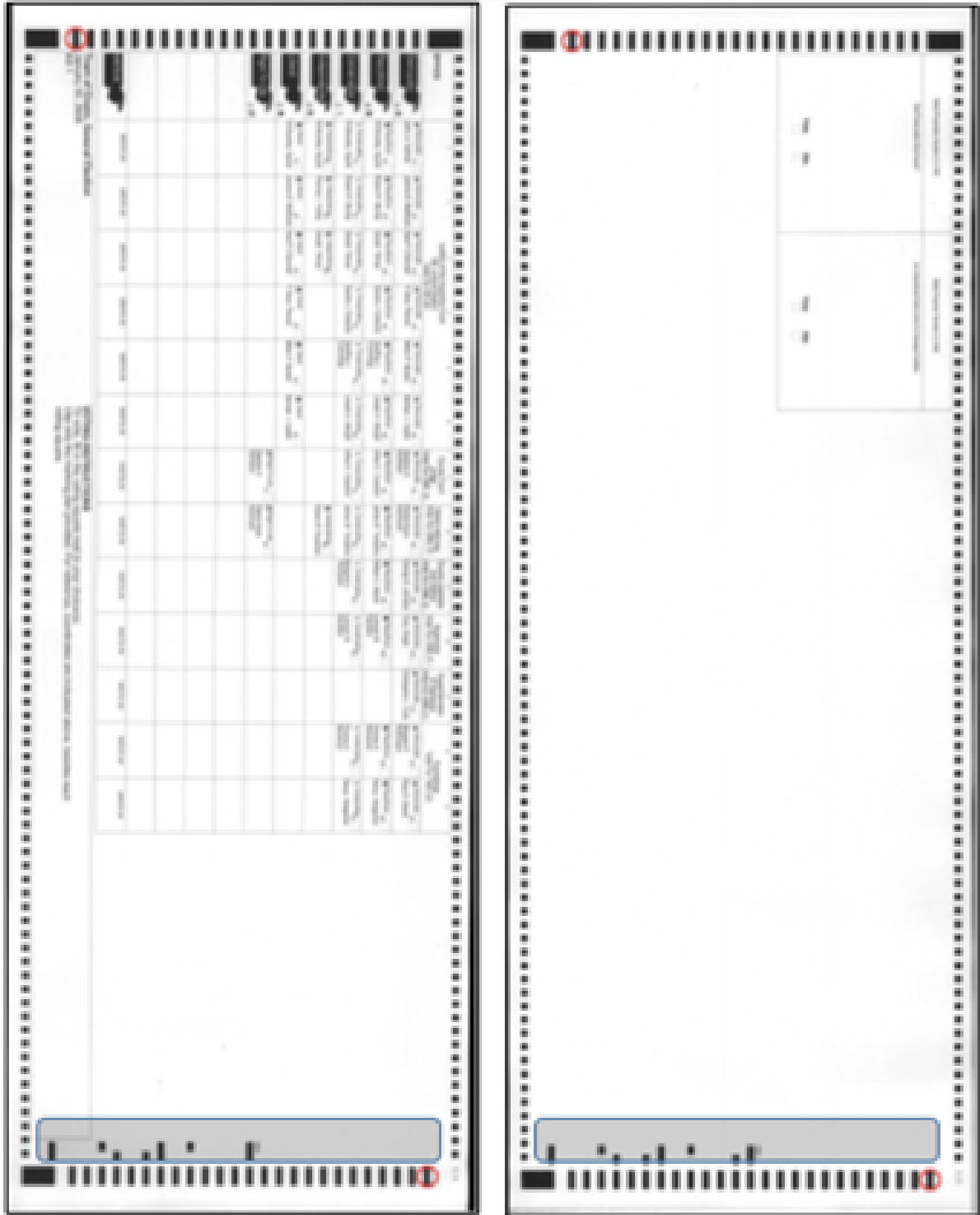


Figure A-3. Dominion (ImageCast election management system)

A.5 Additional information about ballot mark recognition

For all paper-based voting systems, the system counts a mark on a ballot that is in a *sensitive area*:

For a candidate whose name is on the ballot

There is a vote target associated with each choice. The previous sections describe how the targets are found and how they are determined to be marked or unmarked.

Designated for write-in voting for a write-in candidate

A write-in candidate is detected initially during software analysis of the ballot PDF pages to produce the BDFs because the choice names say *write-in*. This initial production of BDFs is always followed by human intervention to make needed adjustments to the files. There may be more than one write-in space for a contest.

The sensitive area associated with a write-in candidate always includes the space where the voter writes in the name. Some ballots also include a voting oval associated with the choice. When the ballot is scanned, if there is no write-in target, a write-in is detected if the write-in area is deemed sufficiently marked. If there is a write-in target, a write-in is detected if the target is deemed sufficiently marked.

For a ballot question

A ballot question is detected initially during software analysis of the ballot PDF pages to produce the BDFs because the choice names are Yes and No. This initial production of BDFs is always followed by human intervention to make needed adjustments to the files.

A voting oval is always associated with each choice, and so scanning and adjudicating ballot questions is exactly the same as for candidates whose names are on the ballot. The difference is the way the results are recorded (for example, there is no party affiliation with the choices).