VSAP

VOTING SOLUTIONS FOR ALL PEOPLE

Voting Solutions for All People Use Procedures for Version 4.0

VSAP-UPM-001

Version 4.0

09/26/2025

VSAP 4.0

Document Revision History

Date	Version	Section/Page	Update Description
06/03/2019	1.1	Document	Initial Publication
07/15/2019	1.2	Document	Miscellaneous updates
10/14/2019	1.3	Document	Miscellaneous updates
11/2/2019	1.4	Document	Miscellaneous updates
12/2/2019	1.5	Document	Miscellaneous updates
1/31/2020	1.6	Section 5. and 10.4.	Updated security procedures
02/03/2020	1.7	Cover page	Finalized certification version; document version number
05/30/2020	1.8	Document	More consistent formatting throughout document; updated graphics and pictures; removed redundant information or added section referral; revised section numbers/headings
07/10/2020	1.9	Document	Updated polling place procedures with system enhancements
8/21/2020	1.10	Document	Updated security procedures
11/19/2021	3.0	Document	Updated template to match corresponding documents; updated References; fixed section referrals; certification version
04/01/2022	3.1	Section 19	Removed references to QMS system; no longer useful during post-manufacturing upgrades.
08/01/2024	3.2	Document	Specify placing the Security Seal on the top seam of the IBB
04/11/2025	3.3	Document	Updated BMD screens and poll reports; updated remake procedure; minor formatting edits
08/22/2025	3.4	Document	• Updated description for VBL

Date	Version	Section/Page	Update Description
			• Updated tabulation procedures for Tally and VBL • Minor formatting and removed redundant information; updated reference mentions • Updated Search BMDs image
09/09/2025	3.5	Section 18.6	Updated physical security requirements and some language regarding BMD Warehouse
09/18/2025	3.6	Section 16	Updated/restructured canvassing information and heading
09/23/2025	3.7	Document	Removed outdated information per SME input; removed outside documentation references and updated various procedures to reflect VSAP 4.0
09/26/2025	4.0	Cover page, headers, and footers	Finalized certification version; updated system and document version numbers

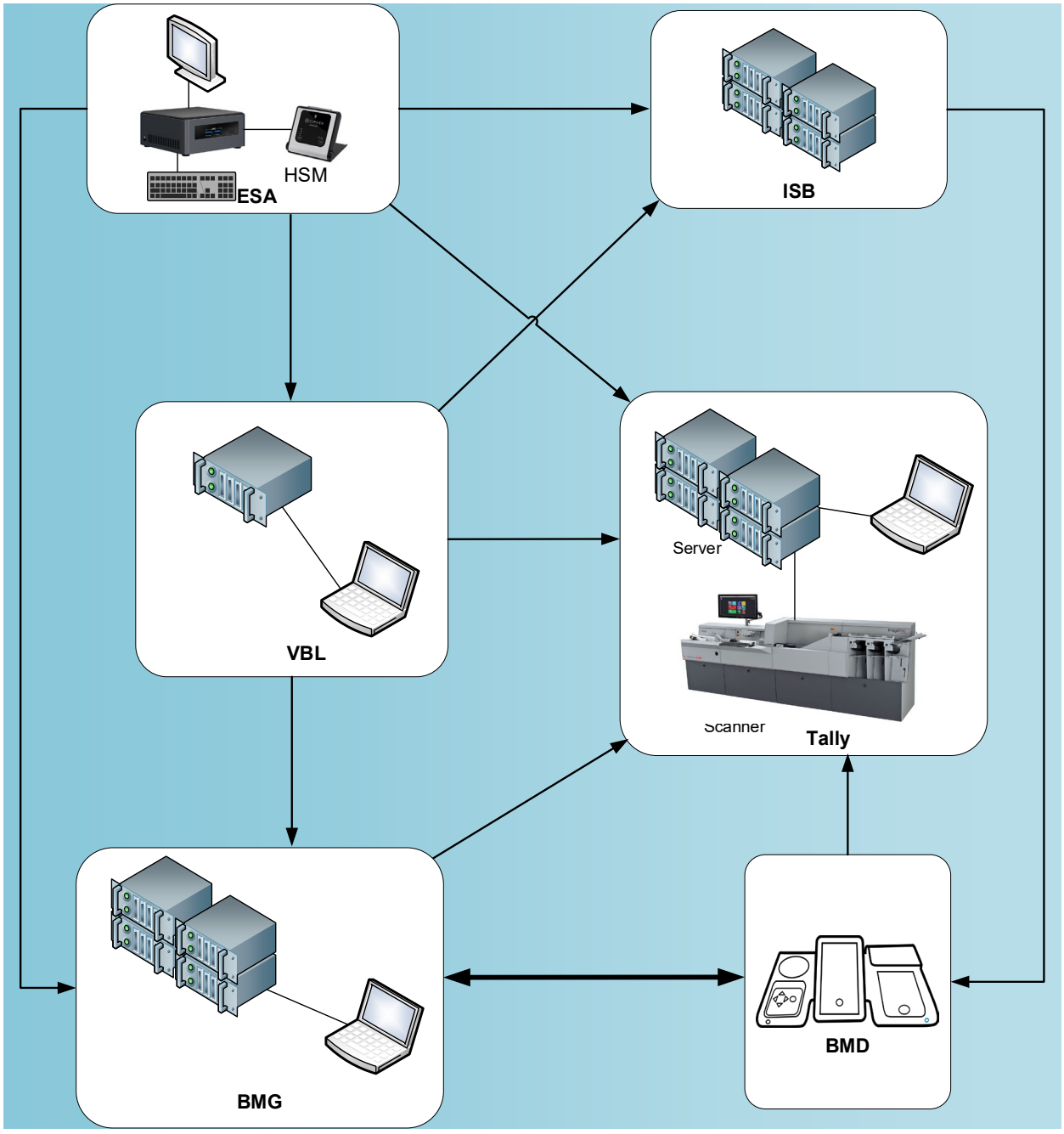
References

Document	Description	Owner	Location
California Voting System Standards (CVSS)	Describes the requirements for electronic components of voting systems	California Secretary of State	https://admin.cdn.sos.ca.gov/regulations/elections/california-voting-system-standards.pdf
Voting Technology Vendors	List of certified voting systems to be used in California	California Secretary of State	https://www.sos.ca.gov/elections/ovsta/voting-technology-vendors/los-angeles-county-vsap
California Elections Code	Laws governing California elections	State Law	https://leginfo.legislature.ca.gov/

CONTENTS

1. Introduction

The VSAP voting system allows voters to engage in elections using interactive technology, mobile devices, touchscreen interfaces, QR code readers, and application-based candidate selection. The system is comprised of six core components: Ballot Marking Device (BMD), BMD Manager (BMG), Enterprise Signing Authority (ESA), Interactive Sample Ballot (ISB), Tally, and VSAP Ballot Layout (VBL). The following section provides an overview of VSAP:



VSAP components

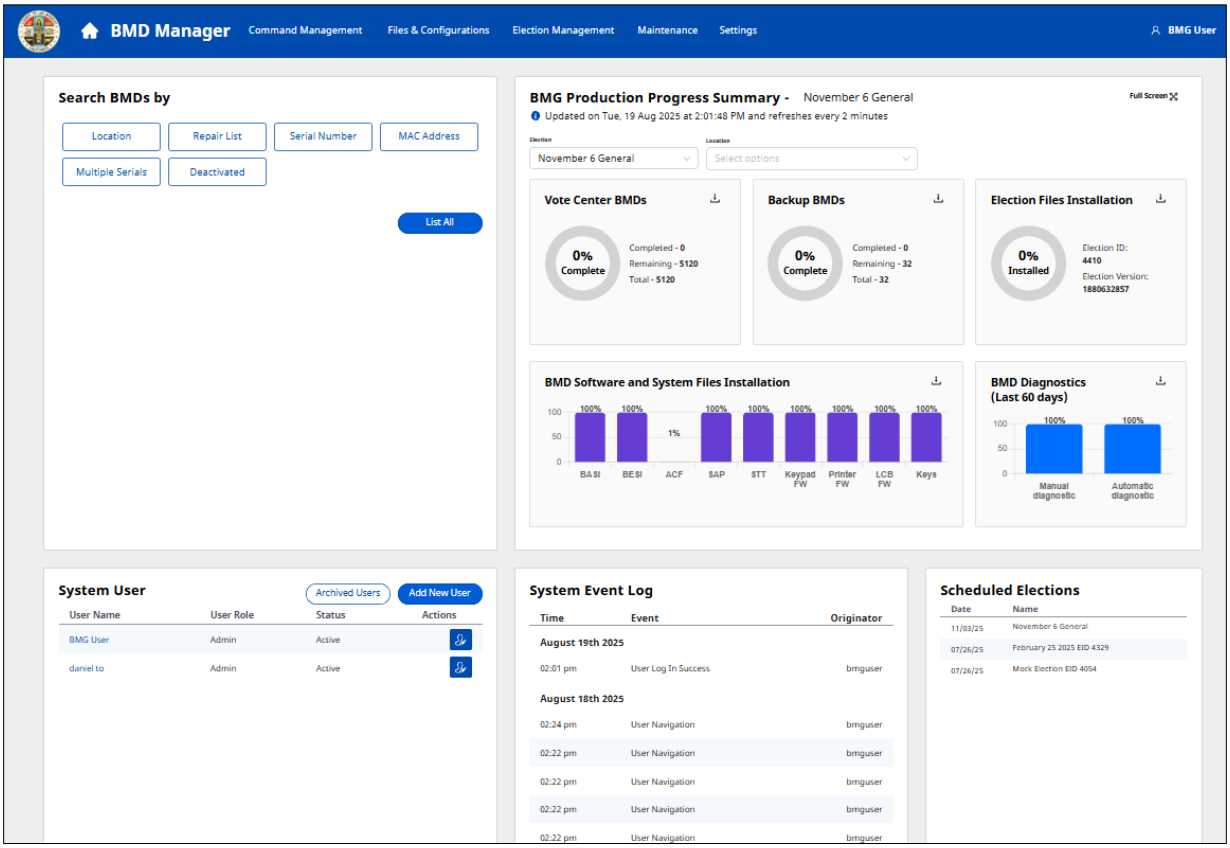
1.1. Ballot Marking Device

The BMD is the primary touchpoint for the voter and hub of the voting system, guiding users with screen prompts and symbols. The BMD features a touchscreen, an audio and tactile controller, and dual-switch input that voters use to generate, verify, and cast a paper ballot. Completed ballots are transferred to the Integrated Ballot Box, which can be detached for unloading. Through the BMD, voters participate in elections.

BMD

1.2. Ballot Marking Device Manager

The BMG manages and maintains the BMDs. It allows operators to manage software, configurations, and data. The BMG provides files necessary for BMDs to present election data such as candidate information, multi-lingual audio, and supporting text. The BMG is the manager and custodian of the voting system.



BMG

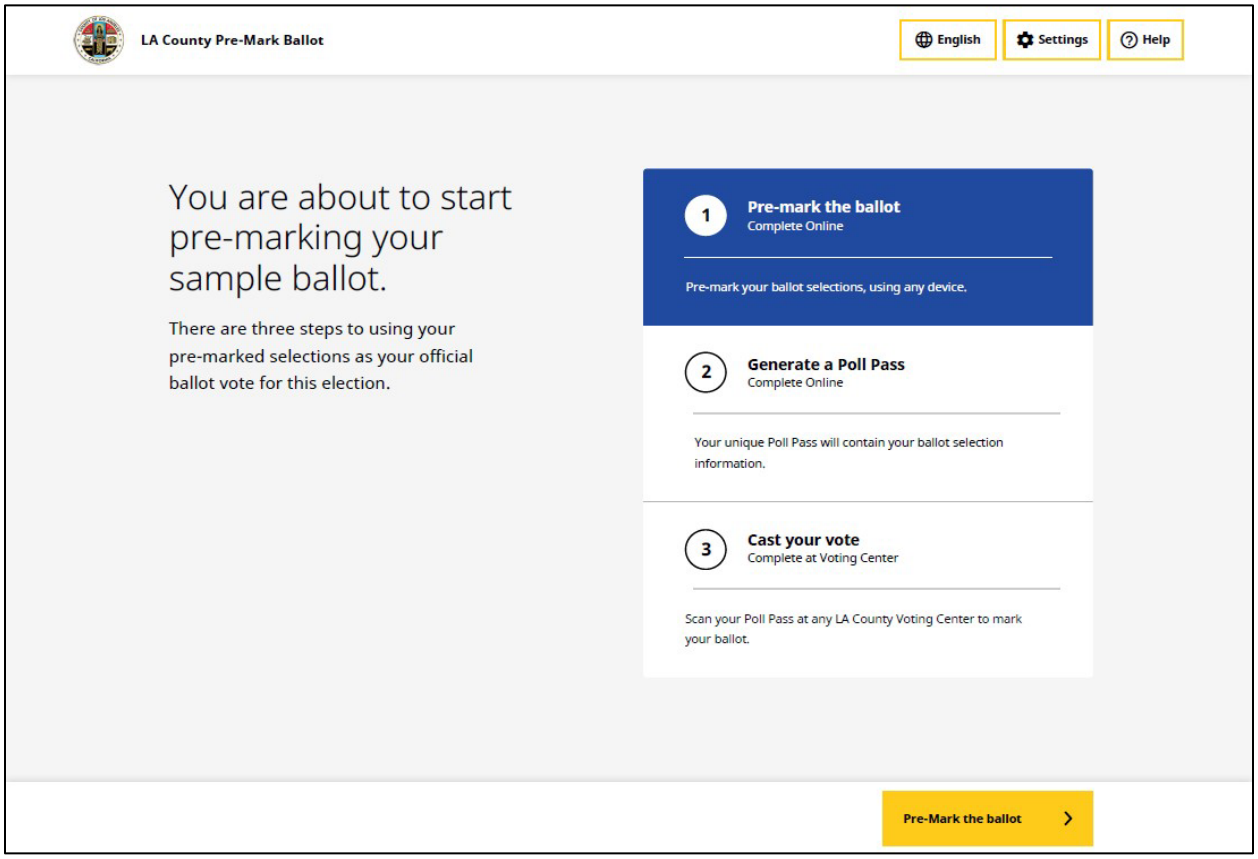
1.3. Enterprise Signing Authority

The ESA establishes the security root and chain of trust for the VSAP voting solution. This subsystem comprises the following processes: key management, distribution, and authentication. The ESA uses a cryptographic module to generate a public/private key pair, which authenticates devices and transactions. The ESA is the basis of the authorization, authentication, and data integrity for the voting system.

ESA

1.4. Interactive Sample Ballot

The ISB is a web-based application that allows voters to mark their selections on a sample ballot, either on their desktop or mobile device, prior to formally voting at a vote center. The ISB generates a Quick Response (QR) code called a Poll Pass, which pre-populates selections in the BMD. The ISB also supports Remote Accessible Vote by Mail (RAVBM) and the Overseas Citizens Absentee Voting Act (UOCAVA). The ISB is what voters use when they interact with the system on their computers or mobile devices.



ISB

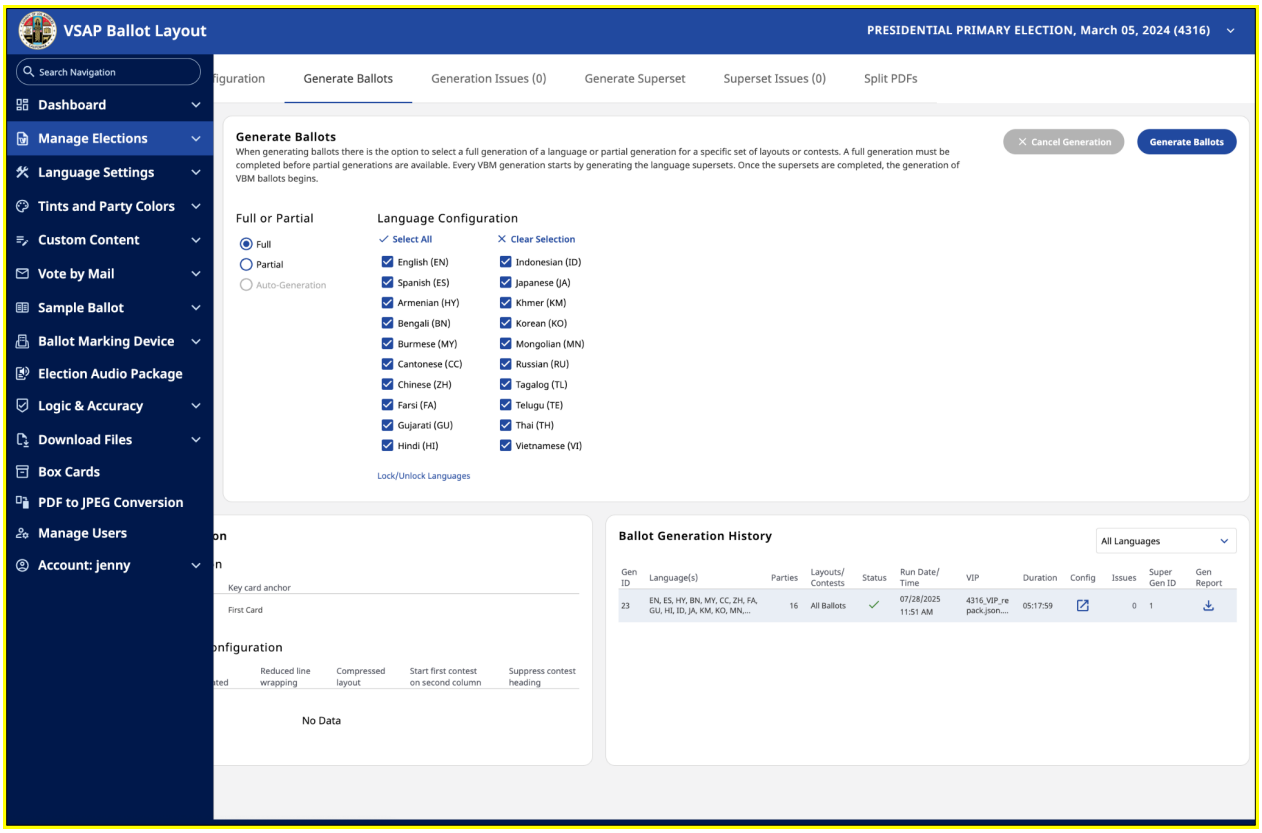
1.5. Tally

Tally captures and processes ballot images to digitally count voter selections from paper ballots. Tally scans and creates images of ballots, converts the images into Cast Vote Records (CVRs), tabulates them, and allows the election results to be exported. Tally is responsible for counting votes at the end of an election.

Tally

1.6. VSAP Ballot Layout

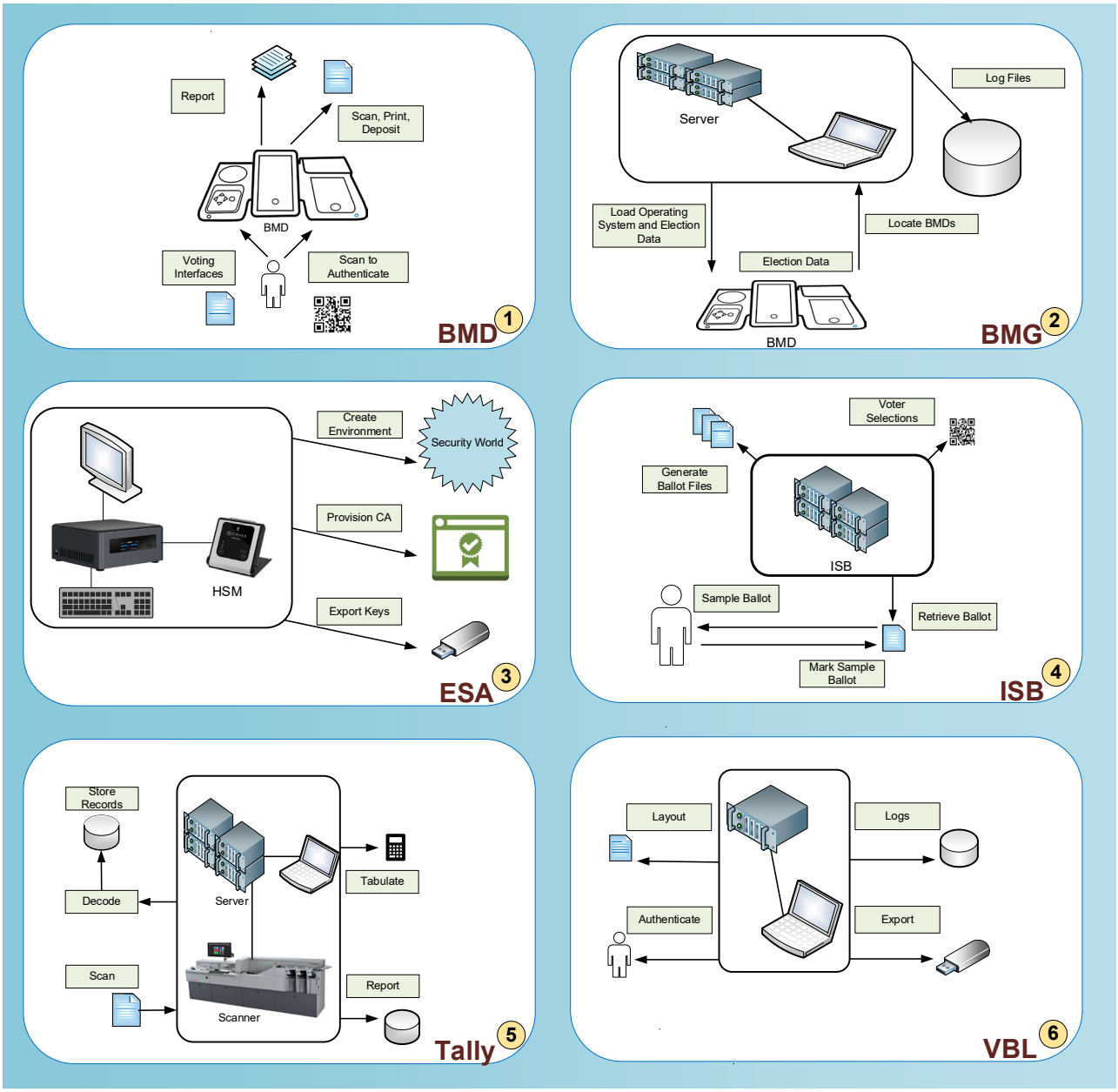
The VBL enables election managers to configure and generate ballot layouts. The VBL system ingests election information files and generates ballot layout files to be used by other components of the system. The VBL makes setting up elections possible. The VBL system generates Vote By Mail (VBM) Ballots and Sample Ballots, which are voter facing.



VBL

2. System Components: Definitions and Descriptions

2.1. Functional Components

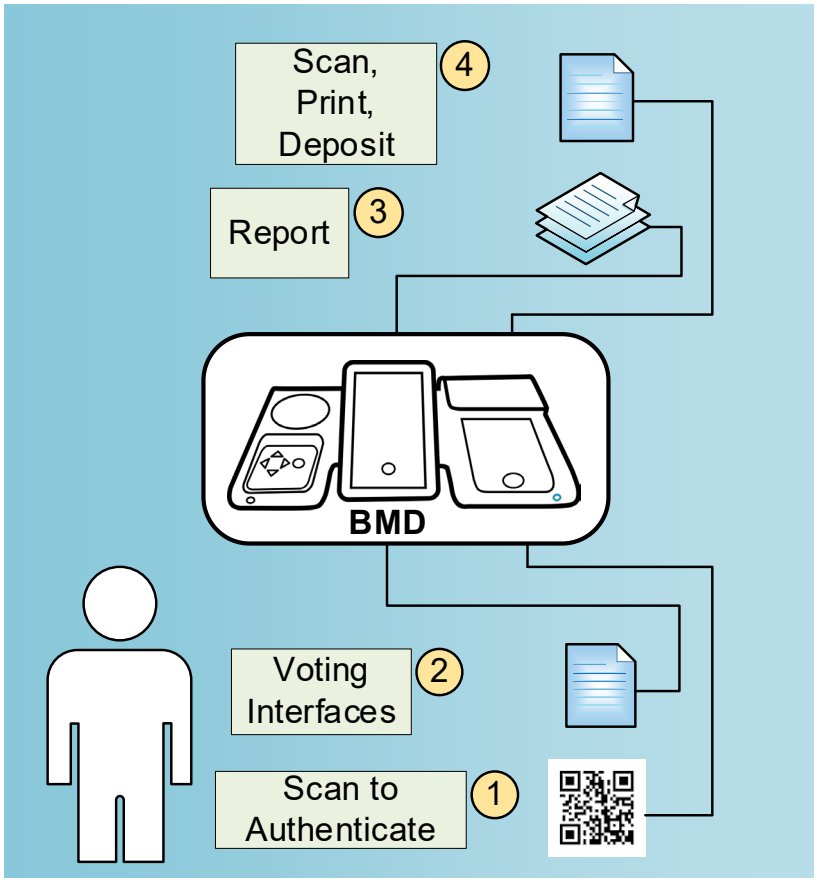


VSAP functional components

Each subsystem of the VSAP system is described at a high level in the following table:

#	Subsystem	Description
1	BMD	The BMD is the primary touchpoint for the voter and the hub of the voting system. It includes a tablet touchscreen interface and several hardware peripherals supporting manual interaction, scanning, and printing capabilities.
2	BMG	The BMG allows operators to manage the software, configurations, and data on the BMDs. Although some diagnostics require manual intervention (e.g., scanner and printer diagnostics, which require paper), the BMG performs automated diagnostics on the BMD without physical access.
3	ESA	The Enterprise Signing Authority (ESA) is a cryptographic module used to ensure each component of the VSAP system conforms to security standards and to validate the data passed to components are secure and authenticated.
4	ISB	The ISB is a digital version of the sample ballot. It is accessible as a web application that permits prospective voters to review election material and mark their selections on their desktop or mobile device.
5	Tally	The Tally system is responsible for capturing and processing ballot images so that voter selections originating from paper ballots are digitally represented and counted.
6	VBL	The VBL system is responsible for defining the ballot print formats for BMD, VBM, RAVBM and UOCAVA ballots, generating data files, audio files, and packages necessary to configure the BMD, BMG, ISB, and Tally, and generating the ballot portion of the sample ballot book.

2.1.1. BMD Functional Components



BMD functional components

At the warehouse, the BMDs are connected to the BMG network using network cables. The BMDs run diagnostics, receive election and configuration files, and download election log files.

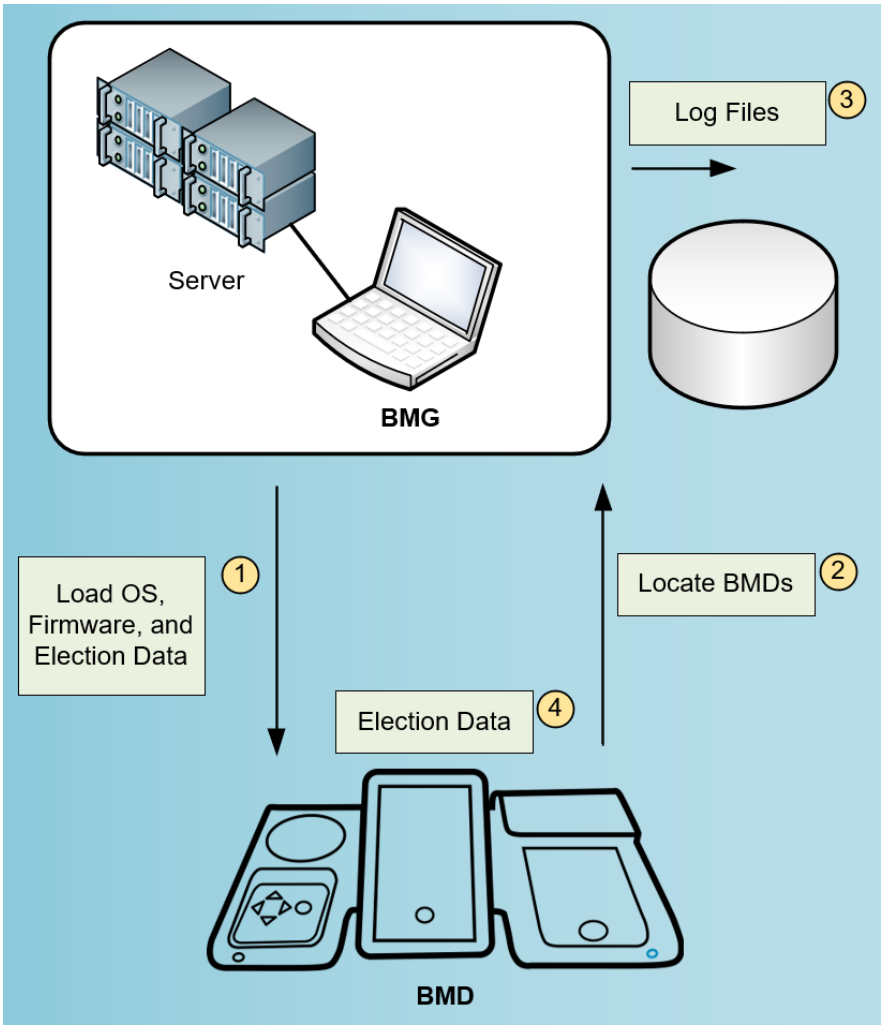
At the Vote Center, an election worker scans an authentication QR code and enters a personal identification number (PIN) to activate the BMD and perform the poll opening procedures. During the voting day, voters receive their ballot from the election workers. The BMD scans the ballot's Ballot Page Meta-data (BPM) QR code containing information used by the BMD to determine the appropriate ballot style to display. After making selections, the voter's ballot is printed with election information, voting selections, and a Selection Barcode Encoding (SBE) QR code containing their selections and BMD information. The voter has an opportunity to review and verify the printed ballot before the BMD deposits it in the ballot box. During the voting day, the election worker empties the ballot box as needed. At the end of the voting day, the election worker performs the poll closing procedures.

Following the election, the BMDs are returned to carts or cases and moved back to the warehouse. Once the BMDs are reconnected to the BMG network, the BMD log files are uploaded to the BMG.

Each function of the BMD system is described at a high level in the following table:

#	Function Name	Description
1	User Authentication	Election workers scan a QR code and enter a PIN for system access
2	Voting	Voters interact with the BMD to mark their ballot selections using various interfaces including the touchscreen, controller, and dual-switch input device; to ensure privacy, headphones provide the audio interface
3	Ballot Management	The BMD scans the ballot BPM QR code, prints the voter's selections and SBE QR code, presents the printed ballot for voter approval, and deposits the approved ballot into the ballot box
4	Reports and Logs	The BMD creates a Vote Center report, election logs, and BMD interaction logs

2.1.2. BMG Functional Components



BMG functional components

The BMD Manager (BMG) manages and maintains the BMDs and allows operators to manage software, configurations, and data.

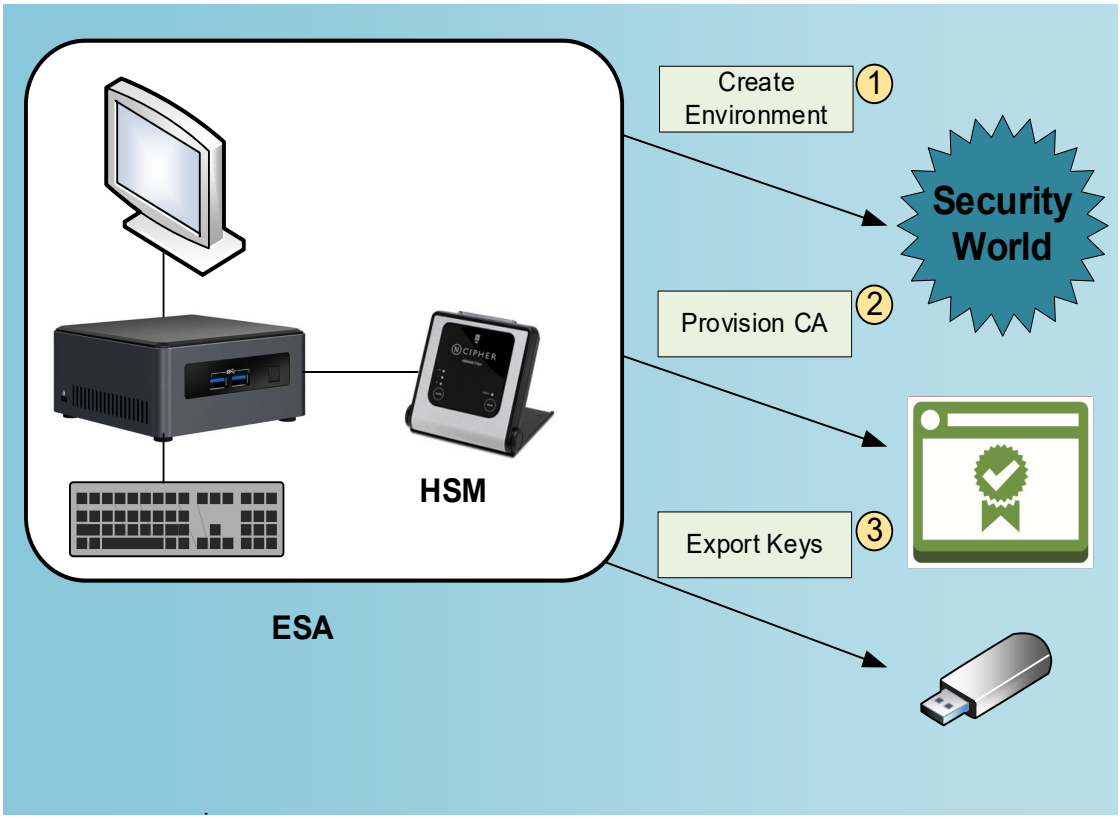
The BMG loads the operating system and the voting application onto the BMDs and conducts system verification. The BMG maintains the location information of the BMDs connected to the BMG network. Processes and interactions are logged. Additionally, the BMG also runs automated diagnostics of the BMDs.

Pre-election, the BMG uploads election data into its repository. The election data can then be loaded onto the BMDs that will be provisioned for an election. Post-election, the BMG downloads the public key files and the log files from the BMDs.

Each function of the BMG system is described at a high level in the following table:

#	Function Name	Description
1	Dashboard	Displays available elections and their corresponding files to be uploaded to BMDs, along with the status of all BMDs connected to the network
2	Configure BMDs	Initially, the BMG loads the operating system and BMD applications onto the BMDs. The BMG loads election data and configuration data onto the BMDs prior to an election
3	Inventory and Location	The BMG identifies the warehouse locations of the BMDs when they are attached to the BMG network
4	Event Logging	The BMG logs processes and interactions
5	Retrieve Election Data	Following an election, the BMG retrieves election logs, interaction logs, and the security keys from the BMDs
6	Manage Users	Users are listed on this page, which is only accessible to an Admin. The Admin can add, modify, or remove users, as well as control permissions.

2.1.3. ESA Functional Components



ESA functional components

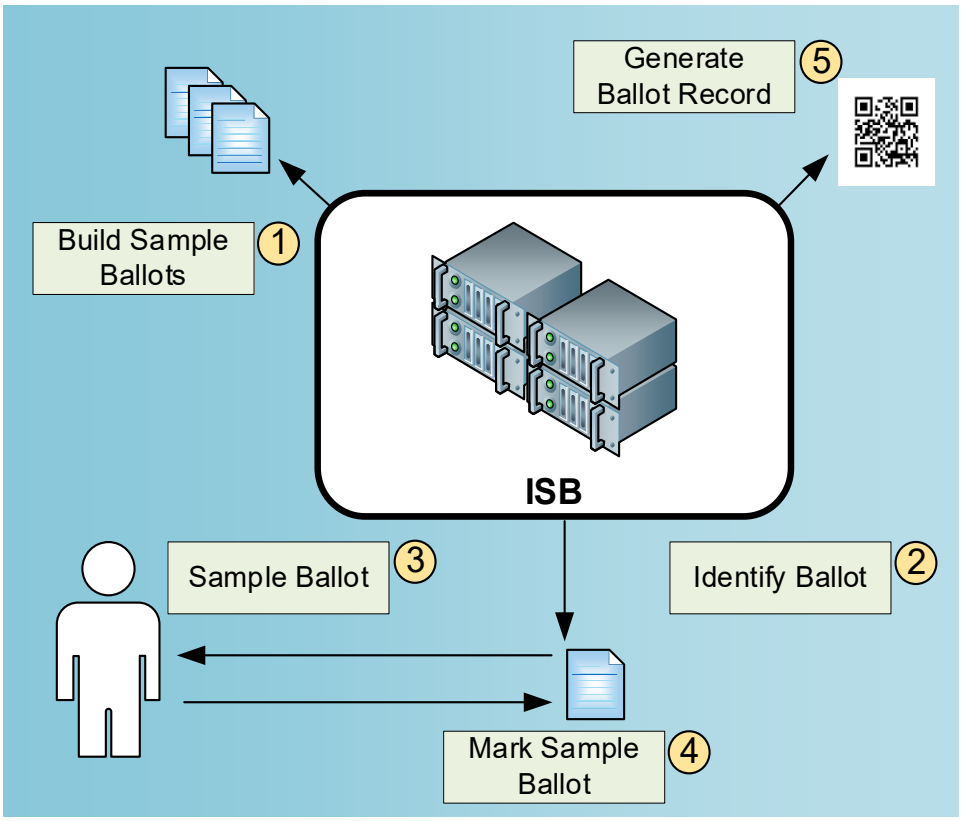
The Enterprise Signing Authority (ESA) subsystem is a cryptographic module used to ensure each component of the VSAP system is conforming to security standards and to help ensure that the data being passed to components are secure and authenticated. The ESA creates a "security world" in the Hardware Security Module (HSM). The ESA sets up sets of operator cards to manage security keys. The ESA provision Certificate Authorities to establish the security root and chain of trust using a cryptographic module to generate a public/private key pair. Once this process is completed, the ESA generates public/private export key pairs for each component (VBL, ISB, BMG, Tally and the Trusted Environment), encrypts each key with its private key, and exports the keys for use in their target servers.

Each function of the ESA system is described at a high level in the following table:

#	Function Name	Description
1	Create Secure Environment	The ESA creates a security world and operator cards
2	Provision Certificate Authorities	The ESA creates a single root CA key and intermediate CA keys

3	Generate and Export Keys	The ESA creates server keys that are exported to target servers in an encrypted state

2.1.4. ISB Functional Components



ISB functional components

The Interactive Sample Ballot (ISB) is a software application that allows voters to review and mark their sample ballots, either on their desktop or mobile device, prior to voting at a vote center. The preprocessor takes the input files and generates data packages optimized for the ISB client application. A map assembles the data about precincts, ballot styles, and parties to associate the voter with the appropriate precinct and identify ballot style. The Voter Selection Manager tracks voter selections and enforces legal and business rules.

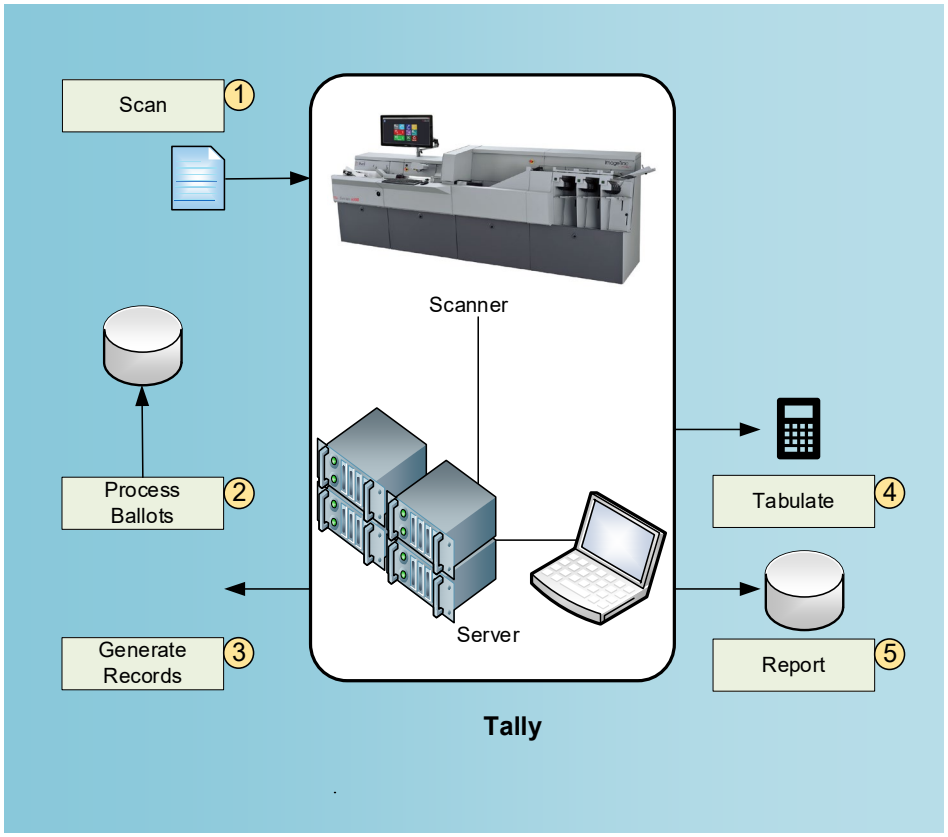
To set up the ISB session, the voter enters either their voter information (last name, date of birth, house number), or address only lookup, allowing the client application to identify the correct precinct and display the appropriate ballot. The voter marks their selections on the sample ballot on their mobile device or personal computer, then reviews their selections. The ISB generates a Poll Pass, which is a QR code representing the selected information. Voter selections can be saved locally on their mobile device for use at the Vote Center to populate their selections onto the BMD via the Poll Pass.

The ISB also enables Remote Accessible Vote by Mail (RAVBM) and Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA).

Each function of the ISB system is described at a high level in the following table:

#	Function Name	Description
1	Build Sample Ballots	Generate data packages for the ISB client application, map precincts to ballot styles, publish ballot files
2	Identify Ballot	The ISB identifies and retrieves the appropriate ballot based on voter information and location
3	Present Sample Ballot	The ISB displays the sample ballot to the voter
4	Mark Sample Ballot	The voter marks their selections on the sample ballot
5	Generate Poll Pass	The ISB generates a QR code with the information about the election, ballot style, and precinct, as well as codes corresponding to the voter selections

2.1.5. Tally Functional Components



Tally functional components

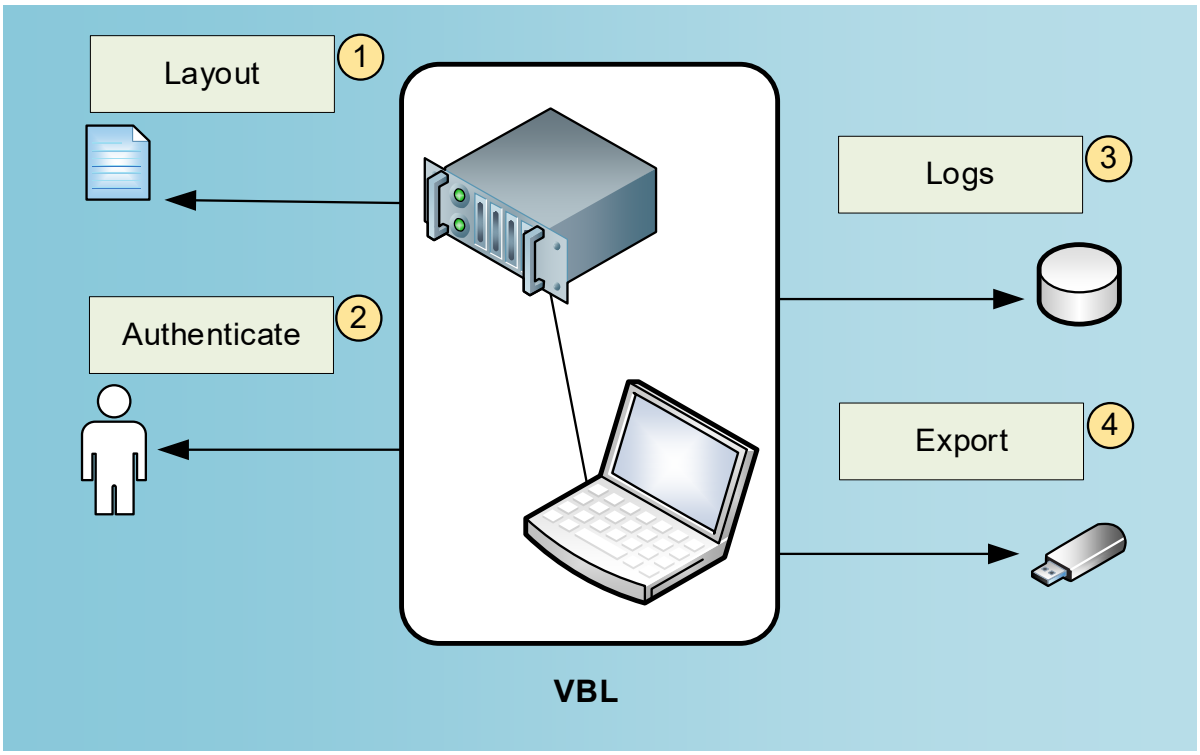
The Tally system is responsible for capturing and processing ballot images so that voter selections from paper ballots (including Full Face and Selections Only) may be digitally counted. There are, from the perspective of the software system architecture, four main Tally processes: (1) Ballots are scanned and images captured; (2) ballot images are converted into Cast Vote Records (CVRs); (3) CVRs are tabulated; and (4) Tabulated results are exported for reporting and auditing.

Each function of the Tally system is described at a high level in the following table:

#	Function Name	Description
1	Scan	The scanning process captures a digital image of each paper ballot
2	Process Ballots	Tally processes the ballots to decode voter intent
3	Generate Ballot Record	The processed ballot data is saved as a tabulation-ready record in the database
4	Tabulate	Records in Tally database are refined and counted to determine election results

5	Report Data	The raw vote data produced by the tabulator is copied to an external database used by an external reporting system

2.1.6. VBL Functional Components



VBL functional components

The VSAP Ballot Layout is an application that enables election managers to configure and generate ballot layouts.

The VBL application supports the logical layout and production of VBM Ballots and election files. These output files provide the rest of VSAP with a definition of the election and ballot layout information. The Auth Service is a standalone authentication service used to manage users, roles, and permissions.

Each function of the VBL system is described at a high level in the following table:

#	Function Name	Description
1	Dashboard	Displays Election Summary, VBL Activities, Activities by Type, and Activities by Language. This is where the users can view running processes at a macro level, as well as current language lock status

2	Manage Elections	This page displays the current VIP defining the election and the VIP import history for that election. The user can import a new VIP on this page, and view VIP Critical Issues, VIP Issues, and Configured Elections. The Configured Elections tab displays All Elections set up in VBL, both active and inactive. The elections listed are quick-links, navigating the user to those election Dashboards
3	Election Settings	All layout settings tied to specific languages are controlled in this section. The user can toggle language locks, view and adjust global and election specific font configurations, download or update custom dictionaries, conduct text layout testing, and surface up ballot contests for high level text proofing
4	Tints and Party Colors	A library of Global Tints that can be used across all elections to register party tints. The user can also assign registered tints to the parties in Election Party Colors for the election in focus
5	Custom Content	A content library where the user can add, edit, and/or configure custom text or images for the VBM, BMD, and/or Sample ballots. Typically this content is used for voter instructions. Election Custom Content is where the user can apply content to the specific election in focus
6	Vote by Mail	Select layout configuration options for the vote-by-mail ballots. Initiate the full or partial generation of vote-by-mail ballots. View generation issues for vote-by-mail ballots
7	Sample Ballot	Select layout configuration options for the Sample Ballot booklet. Initiate the full or partial generation of Sample Ballots to be included in the Informational Sample Ballot (ISB). View generation issues for sample ballots
8	Ballot Marking Device	Select layout options for the BMD's selections-only voter printout. Validate that the desired BMD layout fits on one side of the configured paper size for all supported languages. View BMD validation issues and download Worst Case PDFs
9	Election Audio Package	This page is where the Election Audio Package (EAP) is uploaded and verified by VBL. Issues are surfaced across languages
10	Logic & Accuracy	This page is where the user can configure VBM and BMD L&A decks, in order to generate the necessary artifacts for downstream/ dependent systems like Tally and BMD to validate their functionality compatibility with VBL produced ballots
11	Download Files	Election files, VBM ballots, Supersets, Sample Ballots, and Reports can be downloaded from this section

12	Box Cards	Generate and download box cards for various ballot/box types
13	PDF to JPEG Conversion	Allows a VBL operator to convert a set of PDF files into JPEG
14	Manage Users	VBL users are listed on this page, which is only accessible to an Admin; the Admin can add, modify, or remove users, as well as control permissions

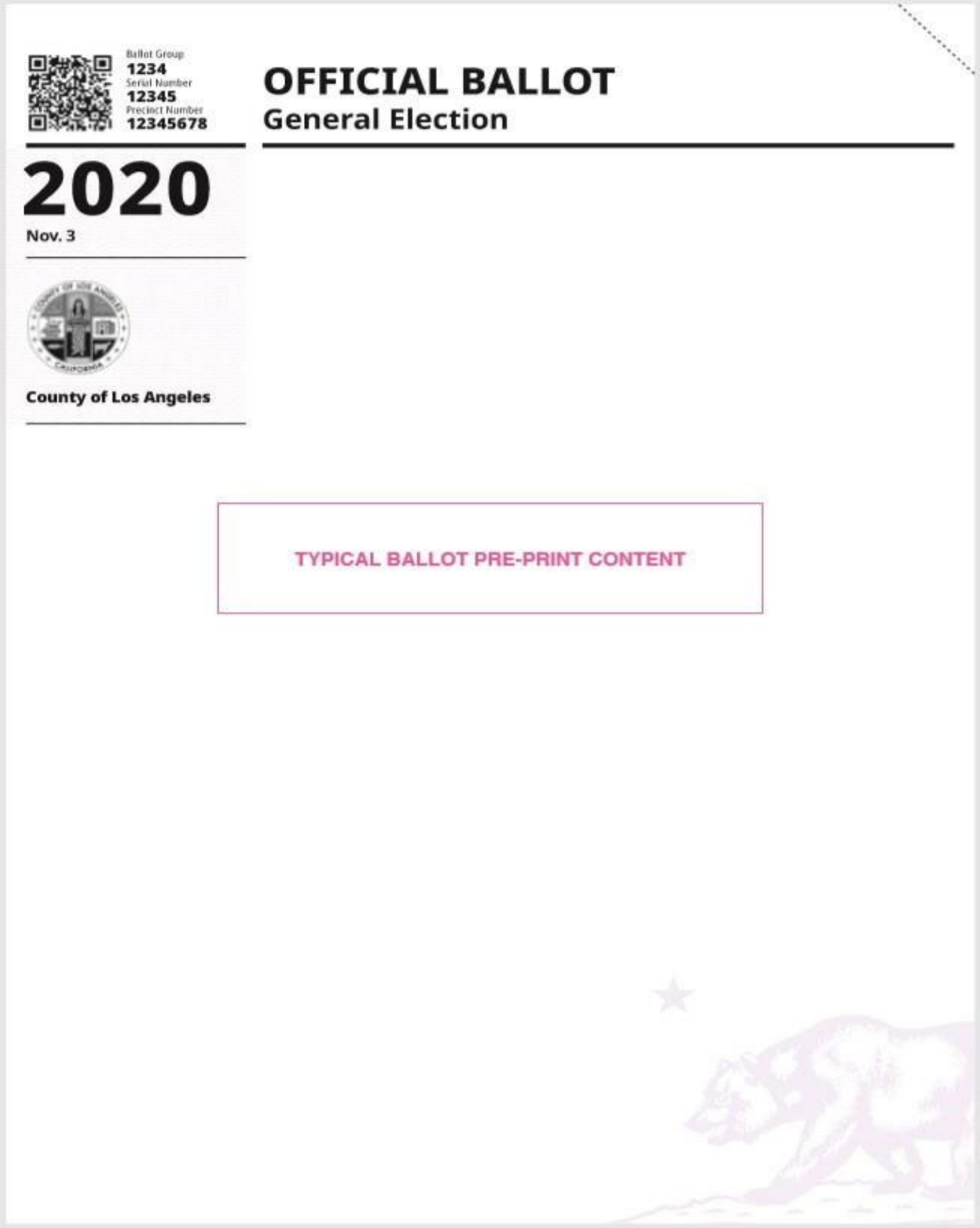
3. Ballot Definition

3.1. Specifications for Thermal Paper

The BMD paper handler uses KANZAN KL 412, Mitsubishi Grade TF 1467, and Mitsubishi Grade T 1633 thermal paper.

Grade	Substance (g/m2)	Caliper (micron)	Sensitivity	Durability (years)
KL 412	131	0.143 ± 0.008	Standard	25
TF 1467	138	0.143 ± 0.008	High	12
T 1633	163	0.174 ± 0.008	High	12

3.2. Ballot Layout and Content



BMD general ballot layout

4. Acceptance Testing

VSAP components must be tested for acceptance through the successful running of the tests specified in the System Test Specification documents. For each component, those documents which detail the tests required to successfully authenticate their acceptance and readiness for use are referenced here.

4.1. Logic Correctness, Data Quality, and Security

Test cases and plans for each sub-system of VSAP ensure logic, accuracy, data integrity, and security of the system. It covers all major components, including BMD, BMG, ISB, VBL, and Tally, with test cases tailored to each system to ensure their reliability and secure operation.

4.1.1. Test Design

Test	Structure	Sequence or Progression	Conditions
Unit Testing	Unit testing isolates the smallest testable parts of a build. Testing is performed on each module or block of code.	Tests written prior to code. All unit tests are run against the build. All tests need to pass before quality assurance testing.	Metrics are collected and reported at the end of every sprint. At the project level, the metrics are used to identify areas of improvement and address them.
Functional Testing	Functional testing checks all documented functions/requirements of the application/product. Functional testing is conducted by feeding inputs and validating expected outputs against observed outputs from the application.	Unit tests for code low-level modules (can overlap with engineering unit testing). Integration testing with other products. End-to-end functional testing for the overall solution, including input from stakeholders. User experience testing by community stakeholders. A selection of people from different parts of the community will document all issues found and will convert the issues to "defects." Testing will be conducted at the end of Engineering Verification Testing (EVT), Development Verification	Metrics are collected and reported at the end of every sprint. At the project level, the metrics are used to identify areas of improvement and address them. Some of the metrics gathered are code coverage for unit tests, velocity, burndown, test progress per sprint, and functional breakdown of defects.

Test	Structure	Sequence or Progression	Conditions
		Testing (DVT), and Production Verification Testing (PVT).	
System Testing	System integration tests are performed on all components. The test cases will incorporate test scenarios that confirm continuity and accuracy across modules and accommodate testing of files produced by or for external systems.	The tests follow the general assumptions for functional tests. The testers validate the input and output of each test and make sure they align with the requirements/stories. The tests cover software, hardware, and any files consumed. Non-functional tests like performance, compliance, accessibility, security, and design validation are also performed at this level. All issues are reported in Jira as defects. Performance tests in this context include scenarios like average response time on the Get and Post APIs. Security tests at this level will be, for example, secure communication between the different modules. Smoke tests are a predefined set of tests that touch critical features of the system. When a new build is delivered to the test team, smoke testing can quickly give feedback to the testers on the status of the build.	Metrics are collected on an ongoing basis and reported at the end of every sprint. They include defect and sprint summary reports with test/pass numbers. At the project level, the metrics are used to identify areas of improvement; they are also discussed during the sprint retrospective meeting with action items for the following sprint. Metrics gathered at the project level are code coverage for unit tests, velocity and burndown charts, and defects found by severity. Additional metrics can be considered if they help the team with continuous improvement.
Integration Testing	Integration test activities are performed on all the components and results from those tests are reported. The test cases incorporate test scenarios	Verify the functional aspects of the integrated system including hardware, software, and consumables.	Metrics are collected and reported at the end of every sprint. At the project level, the metrics are used to

Test	Structure	Sequence or Progression	Conditions
	that confirm continuity and accuracy across modules and accommodate testing of files produced by or for external systems.	Verify the compliance of non-functional requirements such as performance targets and security for this level. Report defects found in the integration tests. Identify solution design problems.	identify areas of improvement and address them. Some of the metrics gathered are code coverage for unit tests, velocity, burndown, test progress per sprint, and functional breakdown of defects.
Hardware/Software Integration Testing	The QA team will verify functional and non-functional requirements of the system using hardware, so that any deviation from the expected behavior is identified to serve as information for possible hardware or software adjustments.	Tests are defined by the QA team and reviewed to ensure they meet VSAP requirements. These reviews are at the end of every sprint or on a schedule established before testing begins.	Defect Summary Report: The defects found in a sprint along with their priority and impact. Sprint Summary Report: Rollup of testing progress for the week, such as the daily report. Daily and weekly Project Level Reports: Determined by the project manager; they may include overall velocity, burndown charts, hot spots, potential problem areas, and/or trending information.
User acceptance Testing	User acceptance tests are performed by the appropriate team using the test suites, test cases, and checklists as well as the information about the	Tests are defined by the QA team and reviewed to ensure they meet VSAP requirements. These reviews are at the end of every sprint or on a	Defect Summary Report: The defects found in a sprint along with their priority and impact.

Test	Structure	Sequence or Progression	Conditions
	required data and environment. Acceptance testing validates that business functions are operating in a manner suited to real-world circumstances and usage. It also gives a chance for stakeholders to review the product before starting production.	schedule established before testing begins.	Sprint Summary Report: Rollup of testing progress for the week, like the daily report. Daily and Weekly Project Level Reports: Determined by the project manager; they may include overall velocity, burndown charts, hot spots, potential problem areas, and/or trending information.
Pre-certification Testing	This testing is integral to the overall successful development of the VSAP solution. The pre-certification testing encompasses both in- and out-of-scope VSAP components.	The first step of pre-certification testing is to ensure all requirements are accounted for in the development process. Certification specialists will be present at scrum meetings to ensure the CVSS requirements are being considered prior to coding. They participate in code reviews to ensure proper coding conventions are adhered to. During the EVT and DVT stages, State-Approved Testing Agency (S-ATA) resources are integrated into the QA teams. As builds are completed, they are verified by the compliance team, and copies of the build are	As builds are completed, they are verified by the compliance team, and copies of the build are provided to the S-ATA for review.

Test	Structure	Sequence or Progression	Conditions
		provided to the S-ATA for review.	
Non-functional Testing	Non-functional testing is performed to check non-functional requirements of the application/product. This testing is conducted by validating expected outputs against observed outputs from the application.	Performance testing Usability testing	As builds are completed, they are verified by the compliance team, and copies of the build are provided to the S-ATA for review.

4.2. Test Details

Test	Test Data (Source, Real or Simulated, Controls)	Expected Results	Evaluation Criteria
Unit Testing	Source: Software specific Type: Simulated Controls: User defined	Verify the functional aspects of the integrated system including hardware, software, and consumables Verify the compliance of non-functional requirements such as performance targets and security for this level Report defects Identify solution design problems	Planning phase is completed System design, technical design, and other relevant documents are properly reviewed, analyzed, and approved Business and functional requirements are defined and approved Testable codes or units are available Test environment is available
Functional Testing	Source: Software specific Type: Real Controls: User defined	Verify the functional aspects of the integrated system including hardware, software, and consumables Verify the compliance of non-functional requirements such as performance targets and security for this level	Unit testing phase is complete Priority bugs found during unit testing have been fixed and closed Integration plan and test environment to carry out integration testing are ready Unit testing for each module is complete

Test	Test Data (Source, Real or Simulated, Controls)	Expected Results	Evaluation Criteria
		Report defects Identify solution design problems	
System Testing	Source: Software specific Type: Real Controls: User defined	Verify the functional aspects of the integrated system including hardware, software, and consumables Verify the compliance of non-functional requirements such as performance targets and security for this level Report defects Identify solution design problems	Integration testing completed successfully Priority bugs found during previous testing activities are fixed and closed The system testing environment is available Test cases are available to execute
Integration Testing	Source: Software specific Type: Real Controls: User defined	Verify the functional aspects of the integrated system including hardware, software, and consumables Verify the compliance of non-functional requirements such as performance targets and security for this level Report defects Identify solution design problems	Stress, performance, and load tests have executed satisfactorily Priority bugs are fixed and closed
Hardware/Software Integration Testing	Source: Software specific Type: Real Controls: User defined	Verify the functional aspects of the integrated system including hardware, software, and consumables Verify the compliance of non-functional requirements such as performance targets and security for this level	Stress, performance, and load tests have executed satisfactorily Priority bugs are fixed and closed

Test	Test Data (Source, Real or Simulated, Controls)	Expected Results	Evaluation Criteria
		Report defects Identify solution design problems	
User acceptance testing	Source: Software specific Type: Real Controls: User defined	Verify the functional aspects of the integrated system including hardware, software, and consumables Verify the compliance of non-functional requirements such as performance targets and security for this level Report defects Identify solution design problems	The user acceptance tests have executed successfully Management has approved user acceptance testing completion Business requirements are fulfilled No critical defects are remaining Acceptance testing signed off
Pre-certification testing	Source: Software specific Type: Real Controls: User defined	Verify the functional aspects of the integrated system including hardware, software, and consumables Verify the compliance of non-functional requirements such as performance targets and security for this level Report defects Identify solution design problems	Hardware and software received. TDP documentation completed User and installation guides completed User defined procedures followed
Non-functional testing	Source: Software specific Type: Real Controls: User defined	Verify the functional aspects of the integrated system including hardware, software, and consumables Verify the compliance of non-functional requirements such as performance targets and security for this level	User defined

Test	Test Data (Source, Real or Simulated, Controls)	Expected Results	Evaluation Criteria
		Report defects Identify solution design problems	

4.2.1. Test Specifications

4.2.1.1. Specifications

Procedures for the verification and validation of overall software performance have been based on CVSS requirements and are included in the test cases. These tests provide procedures for assessing and demonstrating the suitability of the software for election use.

4.2.1.2. Control and Data Input/Output

As multiple features/functions are combined to simulate an election, testing is performed on those sets of features and functions with a set of steps and procedures. The data entry process is defined by the "Steps" section listed for each test case.

4.2.1.3. Acceptance Criteria

The features/functions under test are known before the start of the election and are integrated into the design of the test. When the test is performed, these features/functions are examined and must meet the expected results described in each test case.

4.2.1.4. Processing Accuracy

Every feature and function tested must meet acceptance criteria as described in each test case.

4.2.1.5. Data Quality Assessment and Maintenance

Data quality and accuracy is measured by determining the expected results of the simulation before any voting is performed. Test results are inspected to ensure they match the expected outcome for the specific input. The data is always within the boundaries of the election system, so any maintenance is inherent in the assessment of data quality.

4.2.1.6. Ballot Interpretation Logic

Ballot interpretation logic is defined before the start of the test. The results of the voting and the response of the system to the voting variations are then known beforehand and listed in the "Expected Results" section of test cases.

4.2.1.7. Exception Handling

Exception handling is verified using the test cases that check for correct handling of exceptions. These test cases represent Error or Exception Handling test scenarios, or the exception handling addressed in individual test cases if the possible exceptions are within scope.

4.2.1.8. Security

Security is an overall functionality tested independently of voting variations. The security aspects are tested within individual test cases.

4.2.1.9. Production of Audit Trails and Statistical Data

Statistical data in the form of election results may be used for determining accuracy and data quality. In each election test, all election test results are produced and examined. Audit trail production is an overall functionality that can be tested independently of voting variations. The election results or statistical data tests steps are addressed in an individual test if the tabulation of results are within scope.

4.2.1.10. Procedures for Assessing Suitability for Election Use

Suitability for election use is controlled by the CVSS. All equipment, hardware, and software undergo assessment, and only items that meet the requirements are included in the VSAP system. This determination is based on the design and architecture documentation for each sub-system where requirements are defined and component selection is controlled. The requirements are further evaluated through corresponding conformity matrices.

Supporting materials include system architecture and design documentation, functional specifications, test plans, and test cases for each major subsystem, as well as security architecture documentation. These supplemental documents collectively ensure that the systems meet CVSS requirements and are verified as suitable for election use.

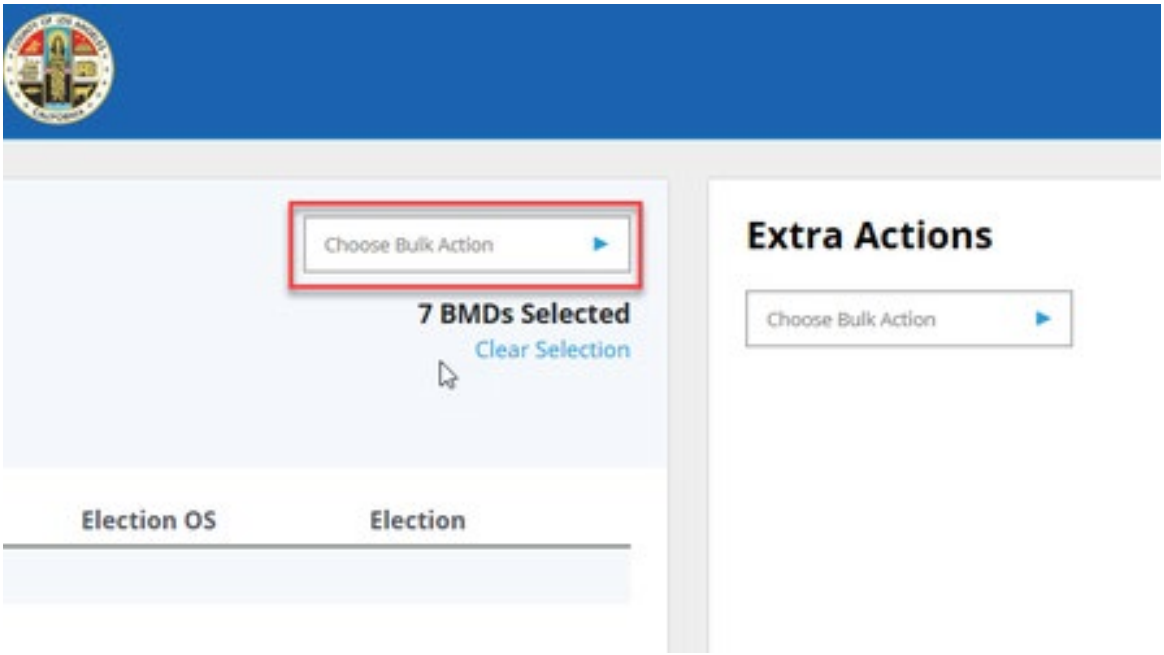
5. System Diagnostic Testing Procedures

Diagnostics can be run on any individual BMD, a filtered group of BMDs, or all BMDs simultaneously using the BMG; the following steps give examples of these features.

1. From the BMG main page, in the Search BMDs by menu, click List All or choose specific search filters to isolate a group of BMDs, or a single BMD

ⓘ A list of BMDs, filtered by your search criteria appears

2. Check the boxes next to any BMD or check the box at the top of the list to select all BMDs



3. Using the first **Choose Bulk Action** dropdown, select **Run Diagnostics**
4. Click Submit

ⓘ You'll be brought to a new page where you'll see a status list of the command you've just run. You'll see either the "SUCCESS", or "FAILURE" test results in the "Status" column, along with details in the "Description" column

6. System Proofing

The components of VSAP must be system proofed to ensure they are working properly and securely. Each component has its own method of system proofing; see below for details.

6.1. Generate VBM L&A Ballot Decks

This process includes generating a Logic and Accuracy deck based on set configurations. It creates archives of generated L&A decks to be retrieved and used for the appropriate testing scenarios on other systems.

6.1.1. Generation Process for VBM L&A Ballot Decks:

1. Navigate to the VBM L&A page from the menu drawer
2. The page displays the current configuration set for Logic and Accuracy. Make sure that this is your desired configuration
3. If not, navigate back to Configure Logic and Accuracy
4. Click the Generate button

ⓘ A message on the Dashboard in Active Processes displays the progress of the generation

5. When generation has completed return to Generate Logic and Accuracy. The configured deck is a new row in the table
6. To access the deck, click the icon in the Create PDF Archive column. This creates a zipped folder on the main VBL server that can be accessed manually following the path defined under Archive Location
7. To convert the deck from PDF to JPEG format, click the icon in the Convert to JPEG column
8. Once the conversion completes, click Create JPEG Archive to create a zipped folder on the main VBL server

Note: The Undervote deck is created during VBM Generation.

6.2. Generate BMD L&A Poll Passes

To execute Logic and Accuracy on the BMDs, VBL produces poll passes following configurable vote patterns. These are produced as sets of PDFs with four poll passes per PDF.

Once the L&A poll passes have been scanned and printed, these selection ballots will then have to be scanned into the Tally system to get tabulated. Tally can then print out the list summary of the test results and compare it to the list summary generated by the VBL system to ensure that the results from the BMD match those of the predetermined totals.

6.2.1. Generation Process BMD L&A Poll Passes:

1. Navigate to the BMD L&A page from the menu drawer
2. The page displays the current configuration set for Logic and Accuracy. Make sure that this is your desired configuration.
3. If not, navigate back to Configure Logic and Accuracy

4. Click the Generate button

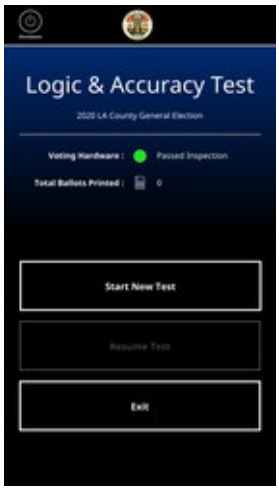
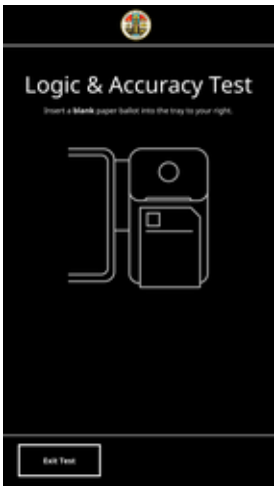
ⓘ A message on the Dashboard in Active Processes displays the progress of the generation

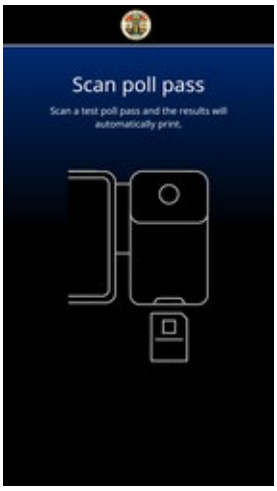
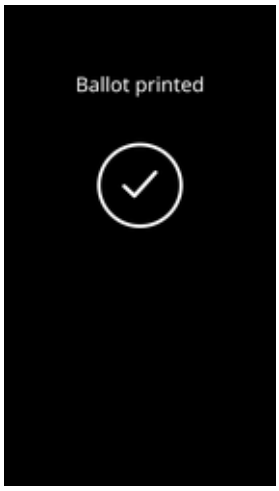
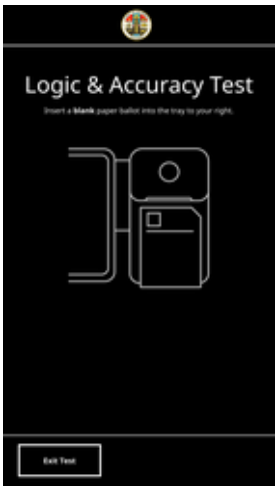
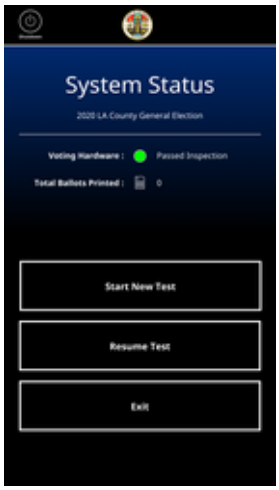
5. When generation has completed return to BMD L&A. The configured deck is a new row in the table
6. To access the deck, click the icon in the Archive column. This creates a zipped folder on the main VBL server that can be accessed manually following the path defined under Archive Location.

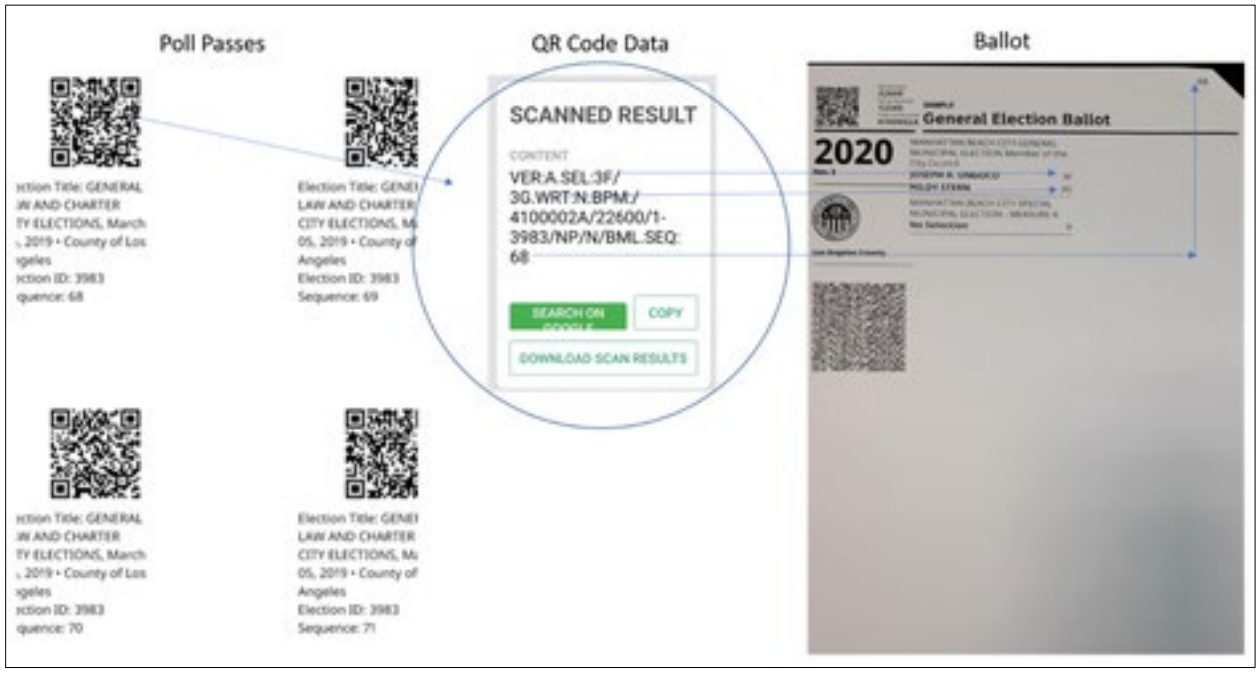
6.3. Using L&A on the BMD

Prior to an election, Logic and Accuracy testing must be done on a BMD to ensure the ballot layouts are correct. To perform this procedure, you need to switch a BMD to L&A mode. Follow the steps below to perform Logic and Accuracy testing using a BMD.

A BMD can't be put into L&A mode if the BMD is in Vote mode. Further, Logic and Accuracy testing can only be done by an election worker whose credentials activate L&A mode. Scanning these credentials automatically puts the BMD into L&A mode, given that the BMD is not in Vote mode.

<table>
<tr><td>1. Scan and enter Credentials, then tap Return To Start.</td><td>2. Tap Start New Test.</td><td>3. Insert a blank paper ballot.</td></tr>
<tr><td> 
</td><td> 
</td><td> 
</td></tr>
<tr><td>4. Scan L&A poll pass.</td><td colspan="2">The ballot prints and drops into the ballot box, then returns to the insert a blank paper ballot page.</td></tr>
</table>

<table>
<tr>
<td> 
</td>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>5. Tap Exit Test to return to the L&A test page.</td>
<td colspan="2">6. Tap New Test to start a new test or tap Exit to exit L&A mode.</td>
</tr>
<tr>
<td> 
</td>
<td colspan="2"> 
</td>
</tr>
</table>



6.4. Lab Test Mode

Lab Tests are used by the Certification Lab to perform the environmental test on the BMD. This mode can be accessed at any BMD and the status can be not open, opened or closed. Only Lab Test Operators have access to this mode. The credentials for the Lab Test are generated in the BMG.

To simulate the Voting Process:

1. Scan and park
2. Print image
3. Eject and hold; repeat

The paper handler test has a counter of how many cycles have been done. During the paper handler diagnostic, all LEDs must turn white and the QR scanner must come on. The time between the cycles must be 10-seconds.

Prior to an election, Logic and Accuracy testing must be completed on a BMD to ensure the ballot layouts are correct. To perform this procedure, you need to switch a BMD to Logic and Accuracy mode.

6.5. Remake Mode

The Remake Mode is used to remake a ballot that has incurred damage and cannot be tabulated by Tally; only Remake operators have access to this mode. The BMG generates credentials for Remake operators. Remake operators can go through the full voting process to reprint voter ballots. The Remake Mode can be activated on any BMD from the voting application.

6.5.1. Activating Remake Mode on the BMD

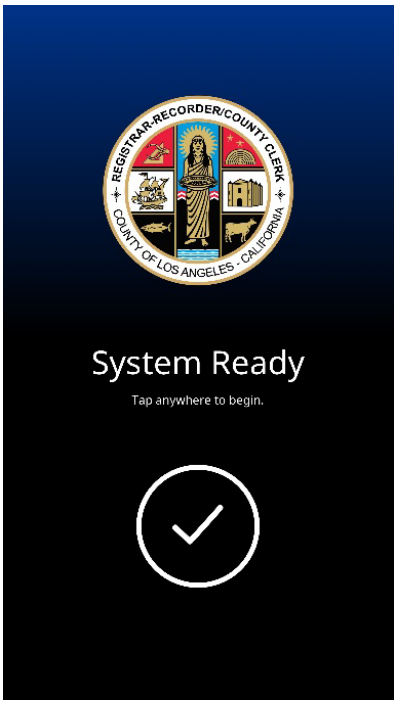
To activate the Remake Mode on the BMD, an operator with the appropriate authorization will scan their two-factor authentication credentials using the bar code scanner to scan their QR Code, then input their PIN using the touchscreen. Authorizations are established within the BMG. The activation is initialized in

either the open or closed poll status. After the operator has entered their proper credentials, the operator will be prompted to insert a blank ballot in the BMD and then must scan the SBE from the unusable ballot. The voter selections will be reviewed.

Note: This information is always in English.

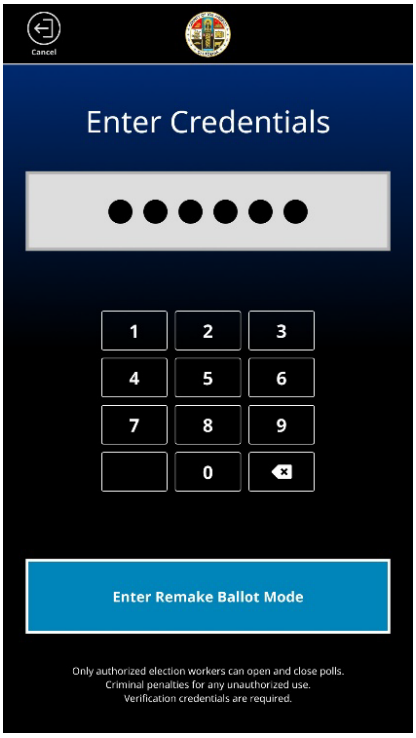
After reviewing the information, a new ballot with a unique ID and sequence number will be generated and then printed. The unique ID is located on the upper right-hand corner of the ballot. All Remake ballots are composed by BMD ID + Sequence.

1. At the **System Ready** screen, tap the touchscreen to start

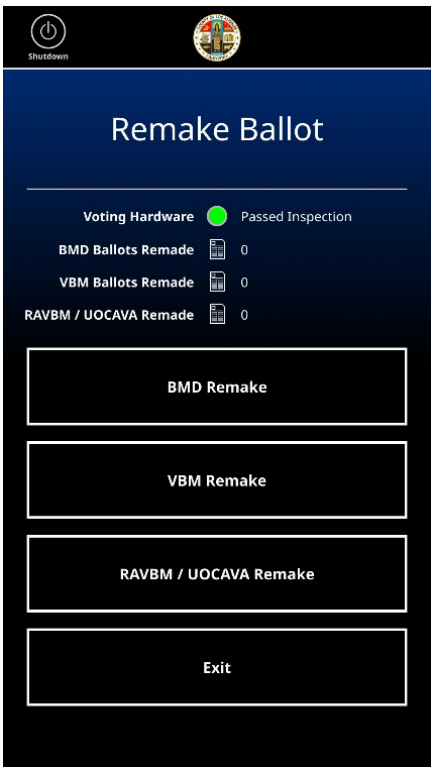


2. Scan **Security Pass** under the right-side of the BMD

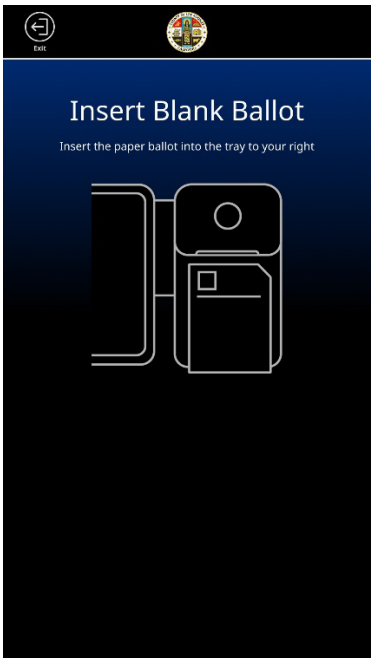
3. Enter six-digit PIN; tap **Enter Remake Ballot Mode**

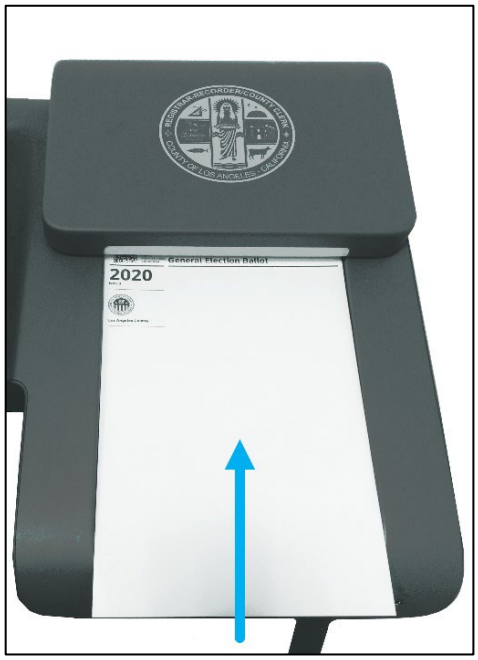


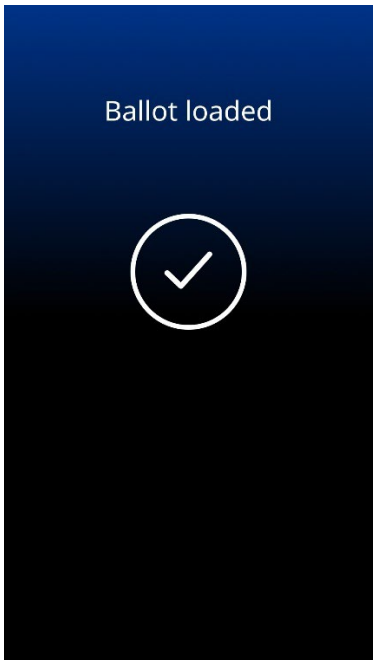
4. Tap **BMD Remake** (it is also possible to remake ballots for VBM and RAVBM/UOCAVA)



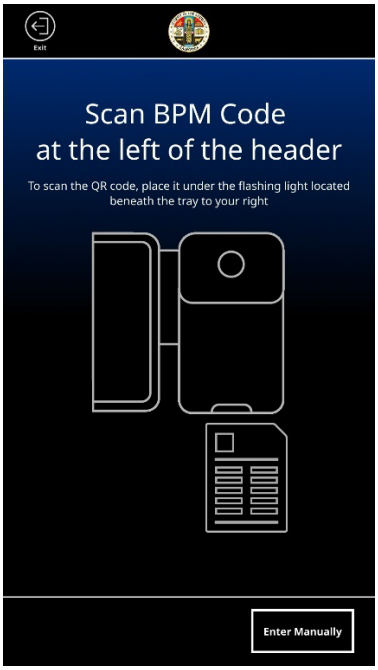
5. Insert a blank ballot into the BMD's paper tray

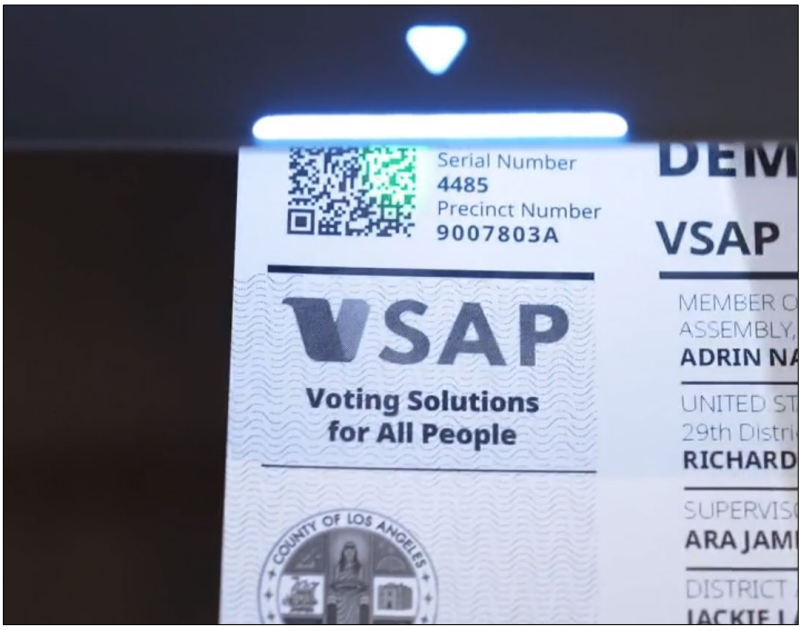




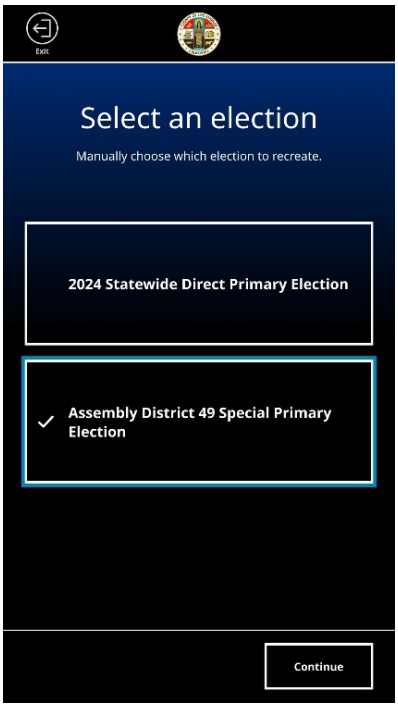


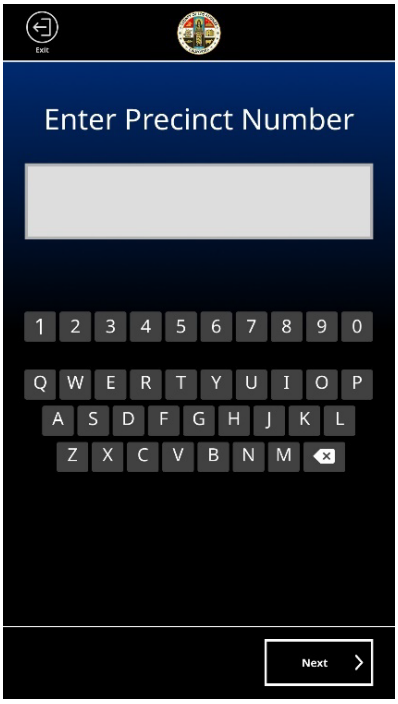
6. Using the **Barcode Reader** located under the right-side of the BMD, scan the **Ballot Page Metadata (BPM)** of the damaged ballot. Scanning the BPM inputs the voter's election, precinct, and party (only for partisan elections), as well as whether the vote is provisional

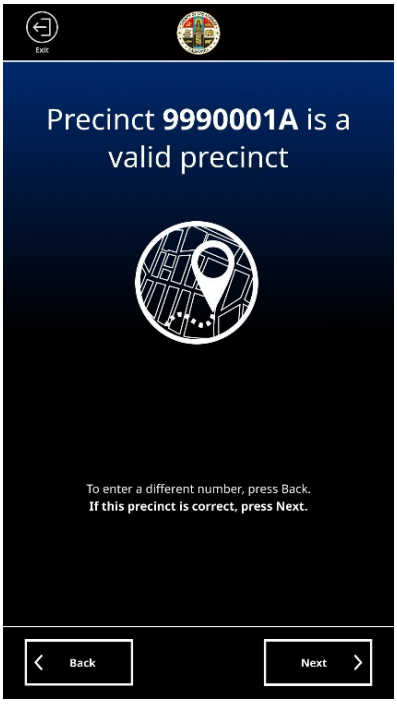




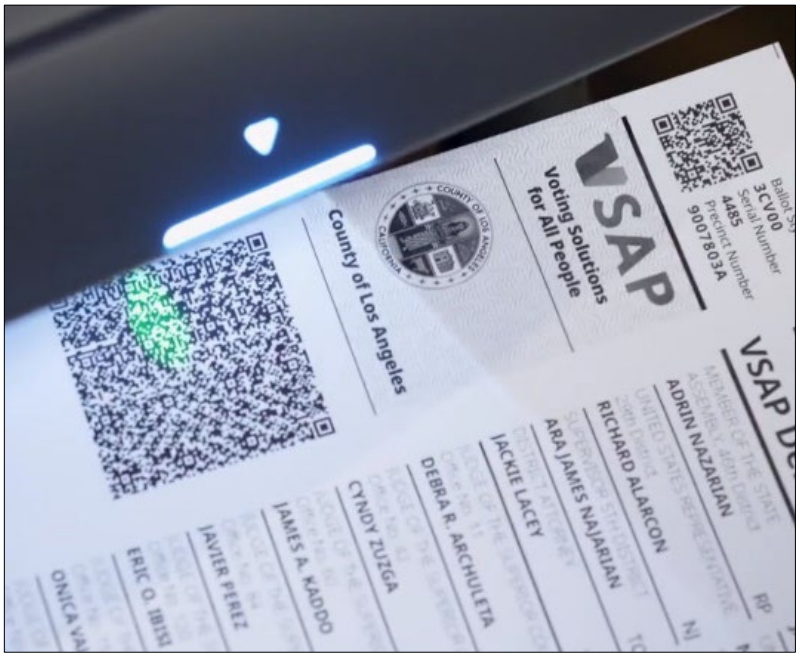
Note: If the BPM is invalid or unreadable, the election, precinct, and party can be entered manually (as shown below):



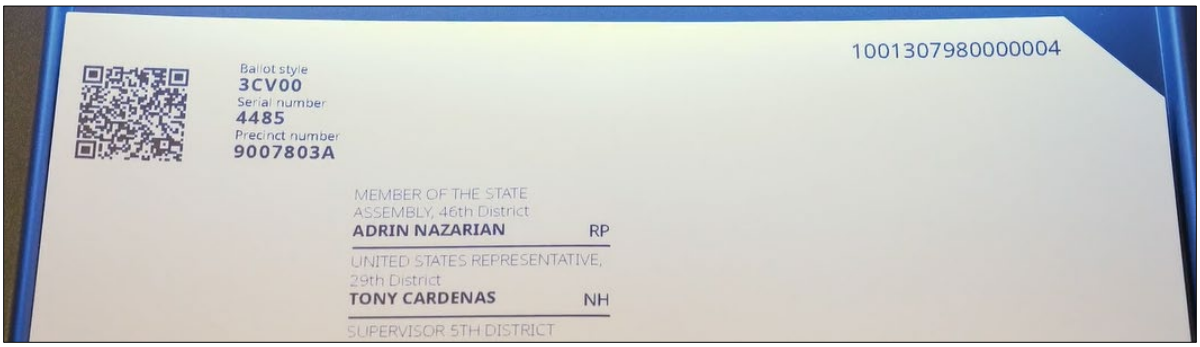




7. Using the **Barcode Reader** located under the right-side of the BMD, scan the **Selection Barcode Encoding (SBE)** of the damaged ballot to transfer the selections; the **Review** screen appears



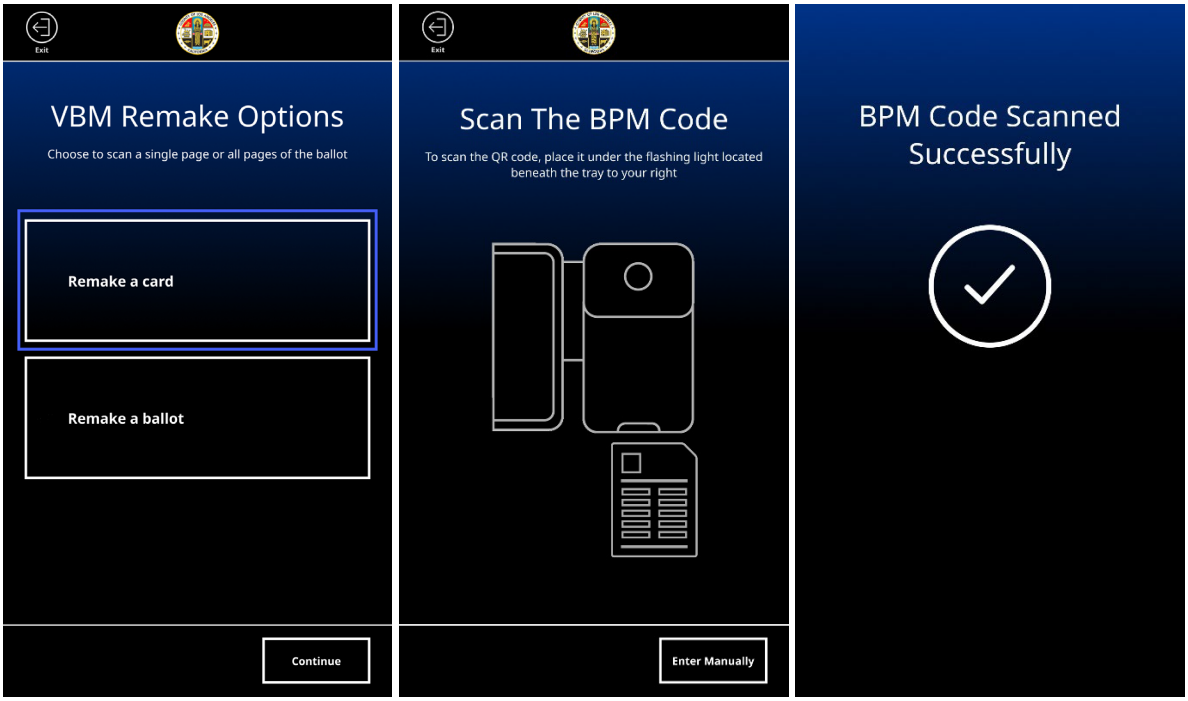
Note: If the SBE is invalid or unreadable, ballot information can be entered manually as referenced in section *Voting Using the BMD Touchscreen*; the ballot is printed with a unique code in the upper-right corner.



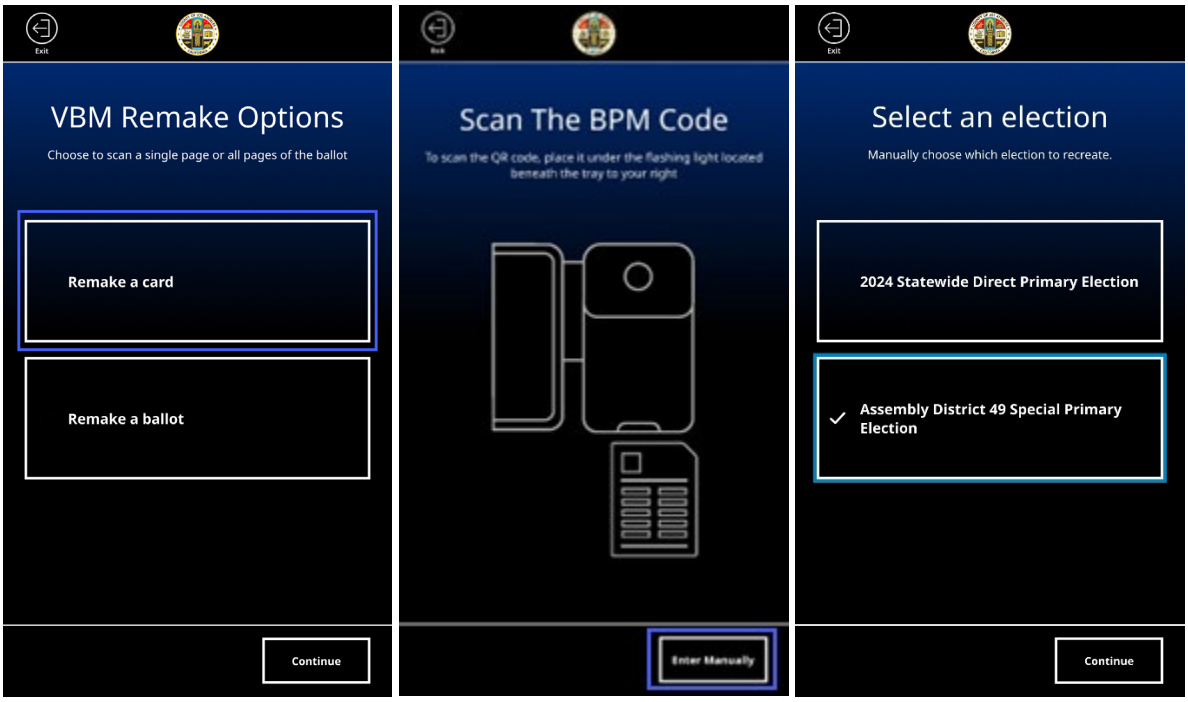
6.5.2. Remake VBM Ballot

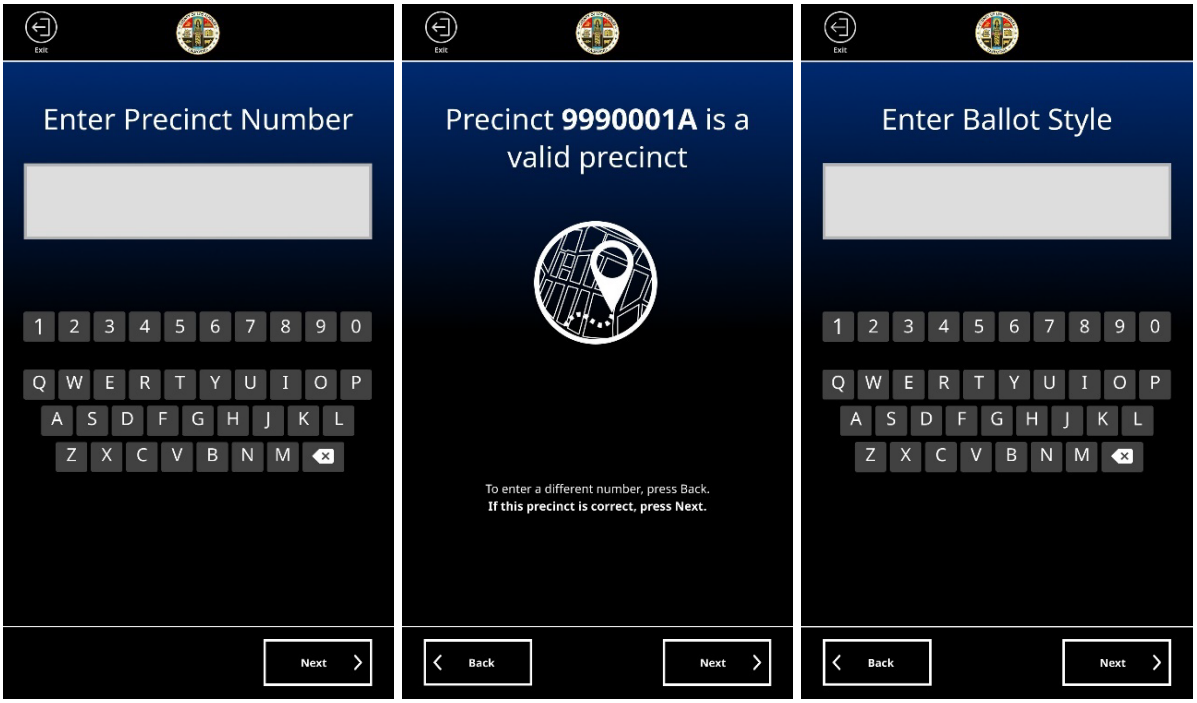
After selecting **VBM Remake** and inserting a blank ballot, choose an option:

Remake a card (Scan The BPM) flow:

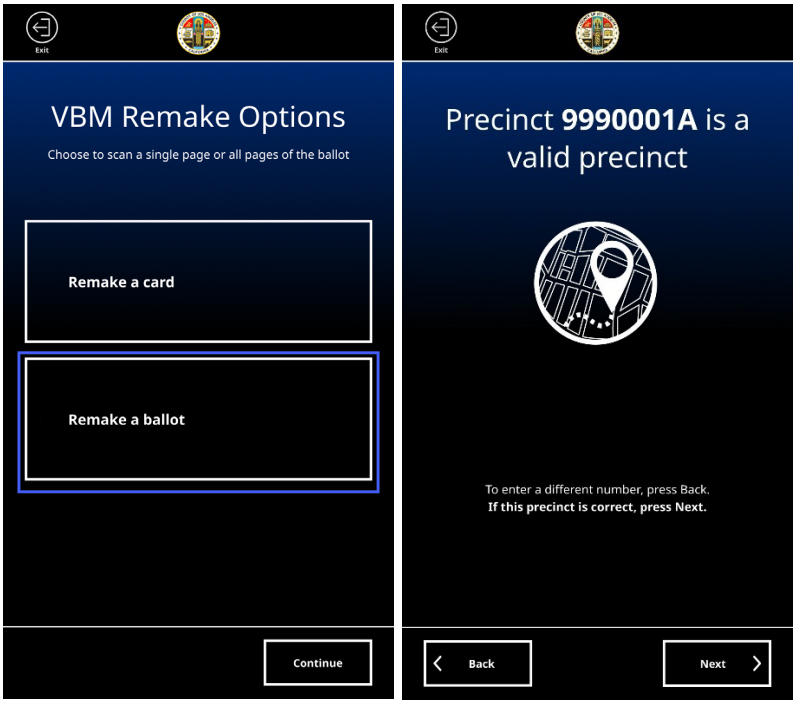


Remake a card (Enter Manually) flow:





Remake a ballot flow:

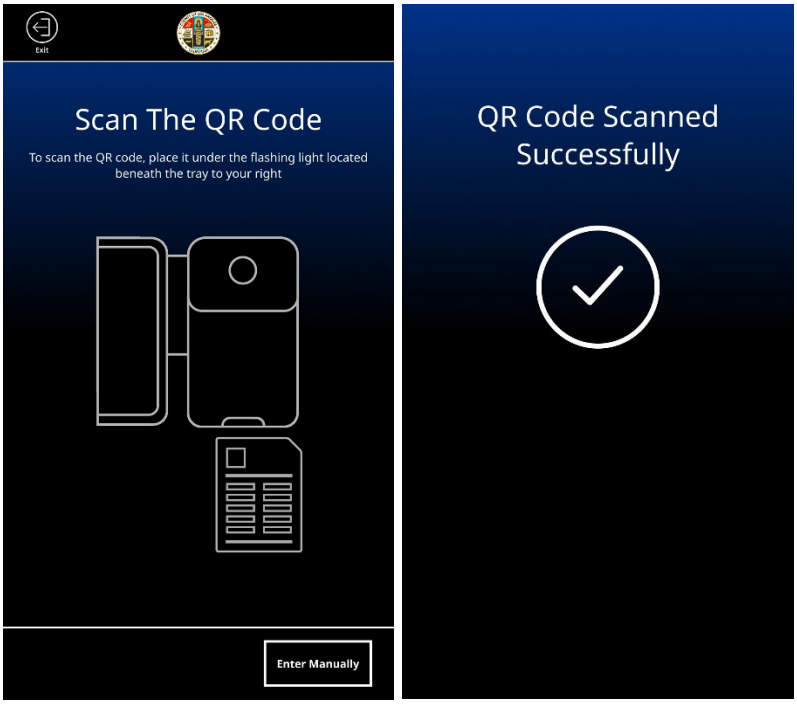


After successfully scanning the BPM code or manually entering the voter's information, the contest screen appears for selections or review.

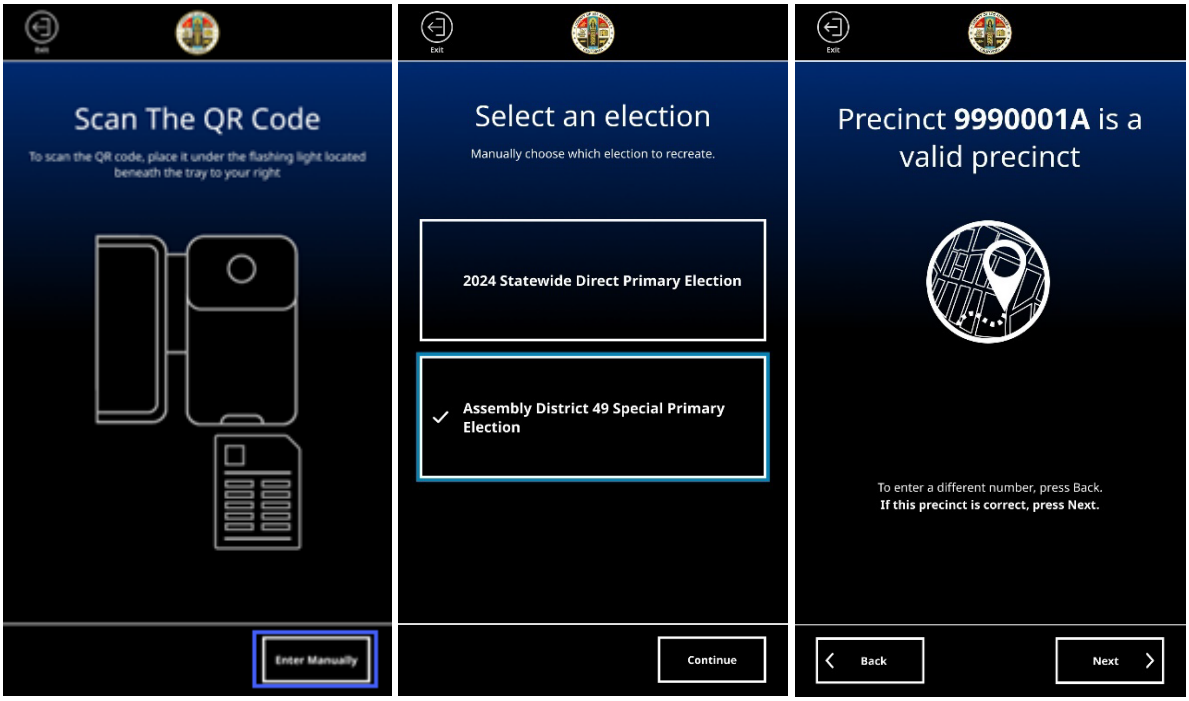
6.5.3. Remake RAVBM and UOCAVA Ballot

After selecting **RAVBM/UOCAVA Remake** and inserting a blank ballot, choose an option:

Scan The QR Code flow:



Enter Manually flow:



After successfully scanning the QR code or manually entering the voter's information, the contest screen appears for selections or review.

7. Multiple Elections

All BMDs are designed to accept multiple elections. When a BMD is loaded with multiple elections, a welcome screen displays the name of all elections configured on the BMD. In this configuration, all activation counters will be stored by the election.

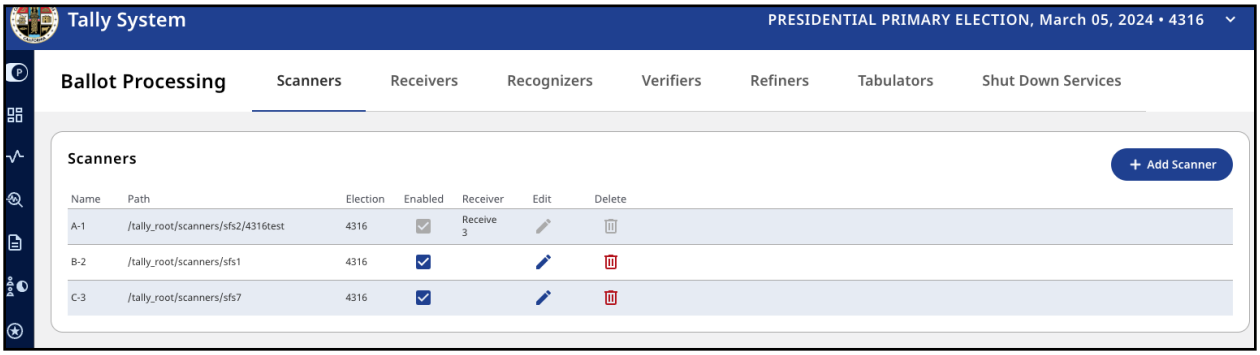
8. Ballot Tally Programs

The Tally Scanners need to be connected to the Tally system and a directory needs to be specified to receive scanned ballots. Follow the directions below to connect a Tally Scanner to the Tally system.

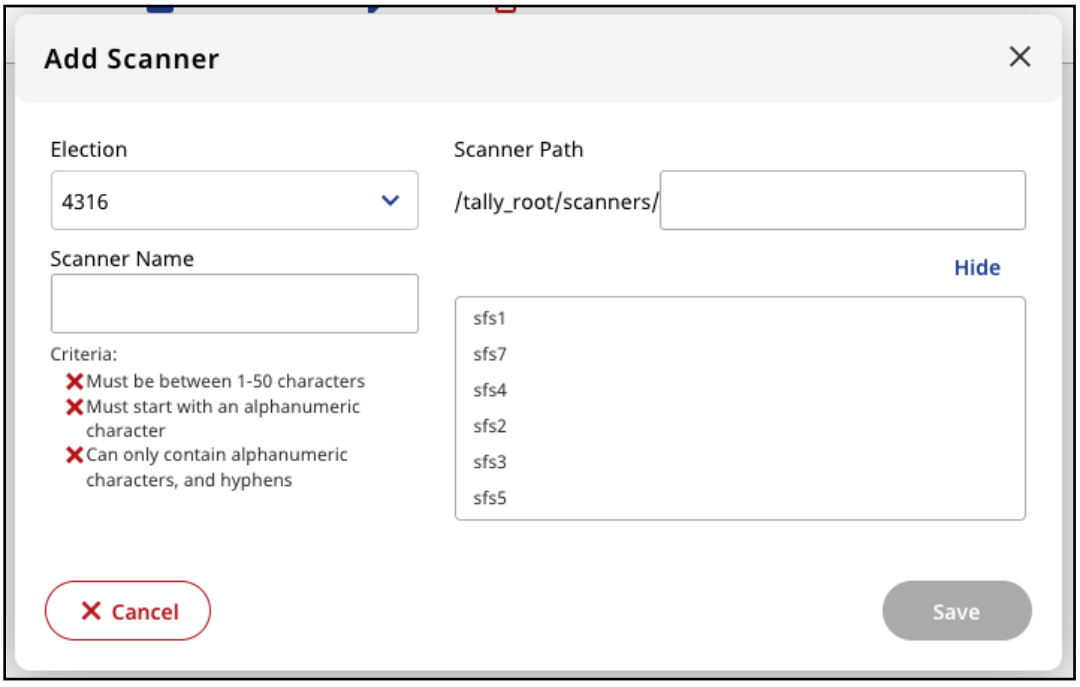
8.1. Tally Connection Process

Once an election is configured, specify which directory will be used to receive the scanned ballot images.

1. From the Dashboard page, select **Ballot Processing** > **Scanners** from the menu



2. From the **Ballot Processing: Scanners** page, click **Add Scanner**



3. Set the scanner name and path to the directory on the file system and select the election to be associated with the scanner
4. Click **Save**

ⓘ Multiple scanners can be configured either for a single election or for multiple concurrent elections

9. Election Observer Panel

The purpose of the Election Observer Panel is to:

- Provide an avenue for public observation of and input into the election process
- Assist in ensuring the integrity of the election process
- Encourage participation and build voter confidence in the election process

9.1. Invitation

Between E-60 and E-30, prepare a media release and letters of invitation to parties likely to participate, such as the following:

- County Grand Jury
- Political Party Central Committee Members
- Advocacy Groups
- Community Based Organizations
- Media
- Other groups or individuals expressing an interest in observing election day activities may also be included in the observer panel, as deemed appropriate

9.2. Appointment Letters

After the groups have provided the names of interested panelists, prepare letters of introduction for the panelists to use when visiting polling places on Election Day. Materials to be prepared for each panelist will include a listing of all polling places within the county for that specific election as well as the central counting site location and hours of operation.

9.3. Mechanism for Feedback

Observers attend training at government facilities, where they can ask questions about the process.

General Rules for Observers

- Observe the proceedings at the polls, including the opening and closing procedures
- Obtain information from the precinct index that is posted near the entrance
- Make notes and watch all procedures
- View all activities at the central counting site on election day
- View the canvass of the vote activities following the election
- View absentee and provisional ballot processing
- Ask questions of staff or voters at the polls
- Ask questions of supervisors at the central counting site

Observer Responsibilities

- Check in at each site, whether polling place or central counting site
- Wear an identification badge
- Maintain a professional manner while observing the election processes
- Ensure they do not interfere with the elections process

Observer Prohibitions

- Interfere in any way with the conduct of the election
- Touch any voting materials or equipment or sit at the official worktables
- Converse with voters (within 100 feet of the entrance to a polling place) regarding the casting of a vote, or speak to a voter regarding his or her qualifications to vote
- Display any election material or wear campaign badges, buttons or apparel
- Wear the uniform of a peace officer, a private guard, or security personnel
- Use cellular phones, pagers, or two-way radios inside the polling place and/or within 100 feet of the entrance to the polling place
- Talk to central counting site workers while they are processing ballots
- Use the telephones, computers or other polling place facilities at polling places or the central counting site
- Touch election personnel
- Eat or drink in the polls or the central counting site
- Assist in operations at any polling place

10. Hardware Maintenance and Preparation for Use

The purpose of this document is to provide the end-user with a maintenance schedule to minimize system component downtime and failure.

10.1. Preventative Maintenance Schedule by System

The routine inspection of system components reduces the risk of major system failures. By implementing a preventative maintenance regimen, minor issues can be detected and addressed before failure occurs and renders the system unusable. The following table lists maintenance items that are usage and calendar based. Perform the maintenance items in the interval or time specified for each system component.

System Component	Action Name	Schedule/Timing	Action/Comments
BMD	Complementary Metal Oxide Semiconductor (CMOS) battery change	Every three years or upon battery depleted indication	Proactive preventative maintenance
	Clean for any spills, dust, other contaminants - before every election	Every election cycle, either as part of pre-LAT or upon equipment return	Clean the BMD touchscreen using a lint free alcohol wipe before and after every election. Spot clean the screen using a lint free cloth every time the ballot box is emptied as well
	Printer	Every time the ballot box is emptied, or every 200 ballots cast whichever comes first	Open the lid, visually inspect for debris, loose printer parts, clean using compressed air and then a lint free, dust attracting cloth to remove any dust; clean the Contact Image Sensor (CIS, internal scanner) with lint free alcohol wipes
	Privacy Flaps	Before every election	Clean for any spills, dust, other contaminants; inspect for visible damage
	Bar code reader	Before every election	Clean using a lint free, dust attracting cloth to remove any dust; check for scratches/damage to the lens
	Ballot box	Before every election	Clean any spills, dust, other contaminants; inspect for visible damage

System Component	Action Name	Schedule/Timing	Action/Comments
	Legs	Every election cycle, either as part of pre-LAT or upon equipment return	Inspect for visible damage; repair/replace if needed
BMG	Archive/back-up, clear logs	Post-election	
	Clean/dust the computing equipment and networking equipment; check any tamper evident seals	Every six months	Do not use canned air or similar, or liquids, on the equipment. Follow County incident response procedure regarding tampered seals
	Run diagnostics	Every six months and 30 days before pre-LAT, whichever is more frequent	
ISB	Archive/back-up, clear logs	Post-election	
	Run diagnostics	Every six months and 30 days before pre-LAT; whichever lends the greater frequency	
	Check AWS Agreements to ensure proper account settings, S3 bucket availability as well as correct expected capacity, and verify configuration of CloudFront (CDN)	Every six months and 30 days before pre-LAT	Per County AWS Agreement
Tally	IBML scanners cleaning	Daily	Recommended IBML operator maintenance
	Fujitsu image scanners Cleaning	Daily	Recommended Fujitsu operator maintenance
VBL	Server Archive/back-up	Post-election	
	Server Clean/dust the computing equipment and	Every six months	Do not use canned air or similar, or liquids, on the equipment.

System Component	Action Name	Schedule/Timing	Action/Comments
	networking equipment; check any tamper evident seals		Follow County incident response procedure regarding tampered seals
	Server Run diagnostics	Every six months and 30 days before pre-L&A, whichever is more frequent	

11. Polling Place Procedures

11.1. Voting Center Supplies, Delivery, and Inspection

This section lists the supplies required to setup the voting location with an emphasis on setting up the BMD.

- Cart containing five BMDs or a case with a single BMD
- BMD peripherals (including stand, privacy shield, headphones, and ballot box)
- Cleaning cloths to wipe the BMD Touchscreen
- Paper ballots shall be in the quantity and manner required by the California Elections Code
- General purpose supplies as provided in the California Elections Code
- Sample ballot booklets of each ballot style if required by the California Elections Code
- Seals and any other supplies and forms
- Tables and chairs
- Power surge protectors
- Power extension cords
- UPS (uninterruptible power supply) if required per jurisdiction procedure

After the carts and containers have arrived, and before the vote center opens, Election workers will perform the following actions:

- Perform a visual inspection of all carts and containers. Inspect and record that all seals are intact on the outside of all carts and containers as per LA County procedure
- Perform a visual inspection of all BMDs. Inspect and record all seals are intact on all BMDs as per LA County procedure
- Set up the BMDs as described in Section 13. Polling Place Procedures

11.2. BMD Set Up

The Ballot Marking Device (BMD) is used by voters to mark and cast a ballot. BMDs will arrive at the Vote Center in carts, with each cart containing five BMDs.

The BMD is comprised of the following components:

- Integrated Ballot Box
- Cross-support bar
- Headphones
- Leg stand
- Power cord
- Power module
- Power module bracket
- Privacy shield
- BMD top module

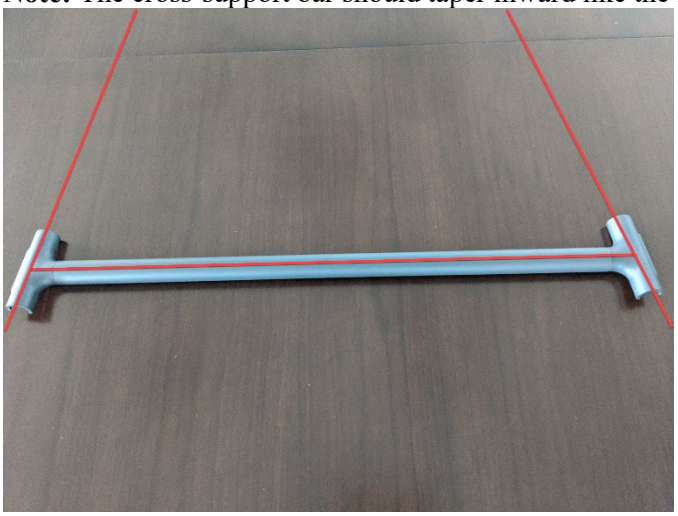
The BMD Technician assembles the BMD using the following instructions:

1. Remove the folded leg stand and cross-support bar from the peripherals container.

2. Open the leg stand by lifting up from the center. Each leg has a spring-loaded feature that allows it to lock securely into place.

3. Line up the grooves on each end of the cross-support bar with the attachment point on the back legs of the stand.

Note: The cross-support bar should taper inward like the letter A.



4. Snap the legs into place, one at a time.

Note: There is a clicking sound indicating the cross-support bar is securely in place.

5. Remove the power module bracket from the peripherals cart.

6. Snap the hooks of the power module bracket onto the leg stand.

7. Remove the power module and the power cord from the BMD cart.

8. Connect the power cord to the base of the power module.

9. Place the power module inside the power bracket.

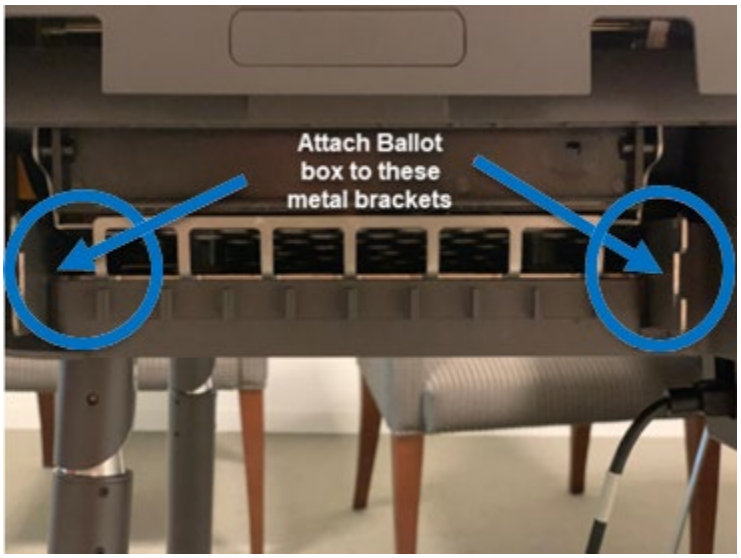
Note: Place the larger power cord in the larger square opening and the smaller cord in the smaller round opening whenever possible.

10. Remove the BMD top module from the BMD cart.
    Note: This is a two-person job

11. Place the BMD top module onto the leg stand by aligning the grooves underneath with the top of the leg stand.

12. Remove the integrated ballot box from the peripherals cart.

13. Attach the integrated ballot box to the back of the BMD top module; to do this:
    - Open the plastic printer cover on the BMD top module
    - Line up the openings on the back of the integrated b**allot box** with the hooks on the **BMD top module**, ensuring the openings are lined up and securely fit together
    - Slide the integrated ballot box onto both hooks on the lower end of the BMD top module, then tilt the ballot box slightly upward to snap it into place



14. Attach and tightly cinch the security zip tie (color may vary) to secure the Integrated Ballot Box; record in the Chain of Custody per LA County procedure. Then place the tamper-evident seal over the seam at the top of the Integrated Ballot Box**;** record the seal in the Chain of Custody per LA County procedure.

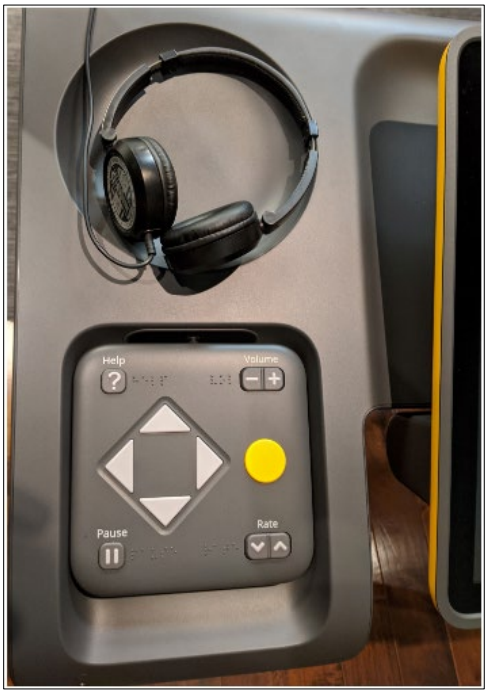
15. Remove the privacy shield from the peripherals container.

16. Unfold the privacy shield and attach it to the slotted holes on the sides of the BMD top module, one side at a time.

17. Gently insert the six-pronged end of the power cord into the socket found on the back of the BMD top module, then plug the power cord into the wall outlet.


18. Remove the headphones from the BMD cart.

19. Place the headphones inside the cradle on the left side of the BMD top module; plug the headphone cord into the port on the back-left side of the BMD top module as displayed.



The BMD setup is complete.

11.3. Additional Ports

Sip-and-Puff/Dual-Switch Device

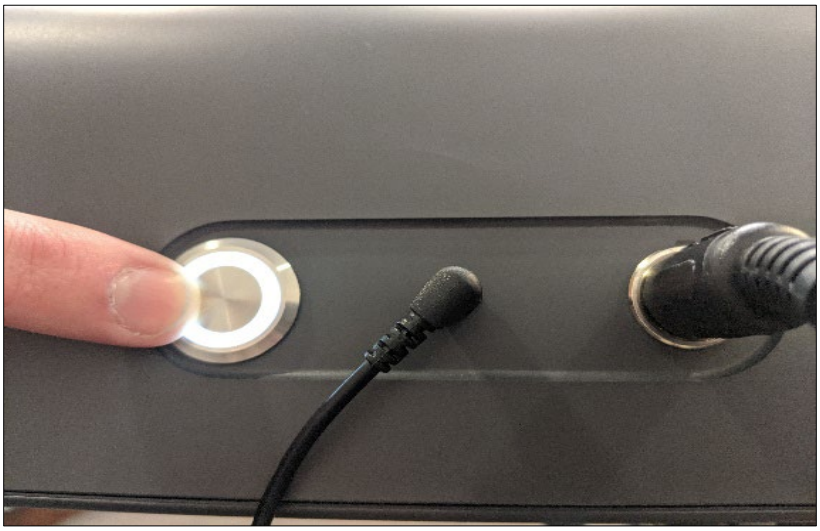
There is an additional port in the lower right-hand corner of the BMD top module that serves as a place to connect personal assistive devices (ex: sip-and-puff or dual-switch).

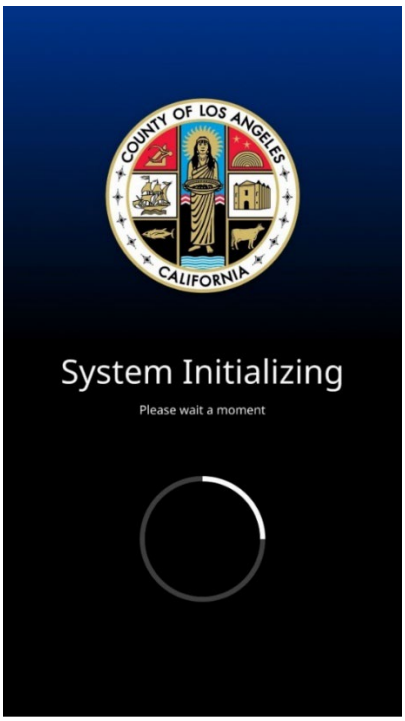
Additional Headphones Port:

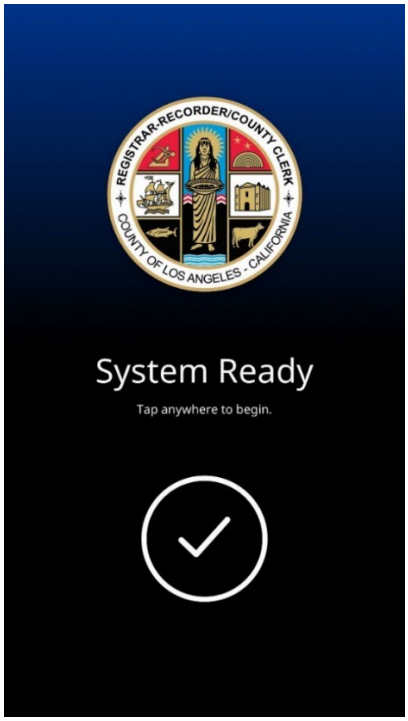
There is an additional Headphones Auxiliary Port on the front of the BMD top module to plug in another set of headphones for another person to assist a voter who's already using the other port.

11.4. Setup Completion

1. Press the Power Button to turn on the BMD.







ⓘ An auto-diagnostics test of the system will occur.

2. In the event the system fails, an error message (#4422) will display on the screen. Shut down the BMD and reboot. If the system fails again after rebooting, the Election Worker will shut down the BMD and report the issue to the Election Worker Lead.

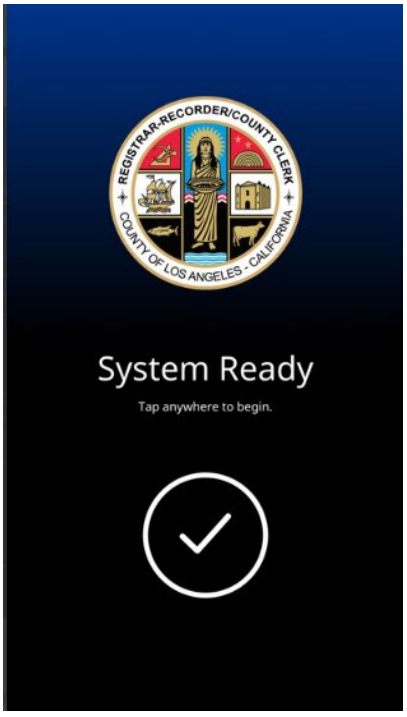
11.5. Opening the Polls

This procedure details how two Election Workers "open the poll" to enable voting on each **BMD**. Opening the polls requires proper security credentials which incorporate a 2-factor security process. These Security Credentials consist of a **six-digit PIN** and a **QR coded security pass,** which are generated by the **BMG** and issued to **Election Workers** per LA County procedure.

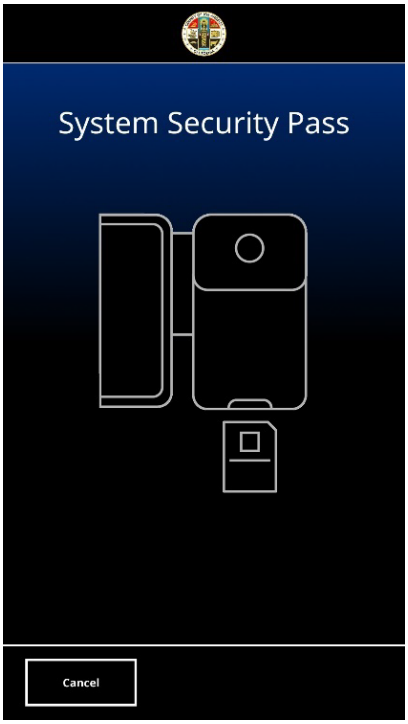
Check the zip tie per LA County procedure. Verify the tamper-evident seal placed over the seam of the Integrated Ballot Box has not been compromised.

1. Press the power button on the back of the BMD

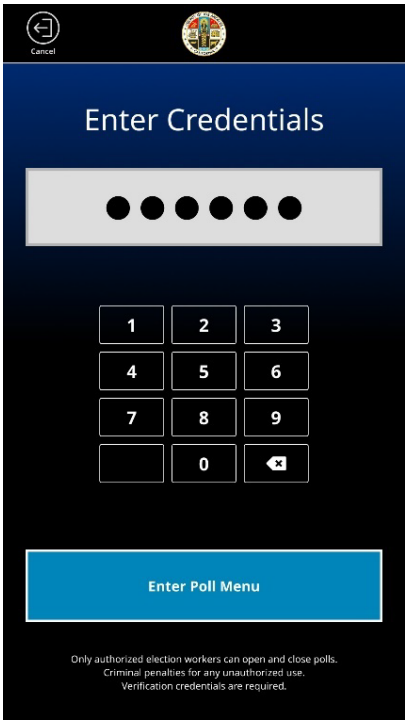
2. At the **System Ready** screen, tap the touchscreen to start



3. Scan the **Security Pass** under the right-side of the BMD



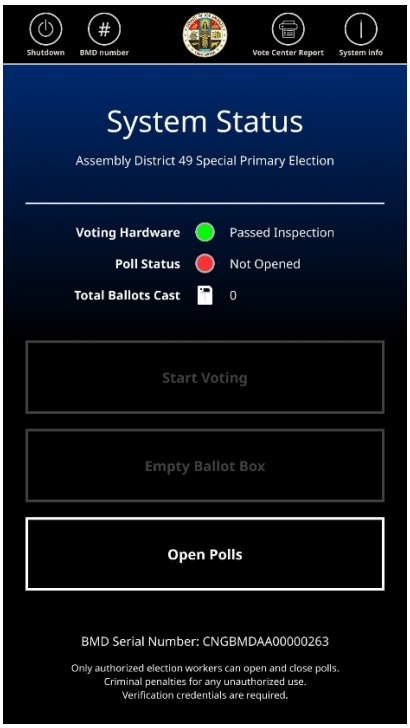
4. Enter the six-digit PIN; tap **Enter Poll Menu**



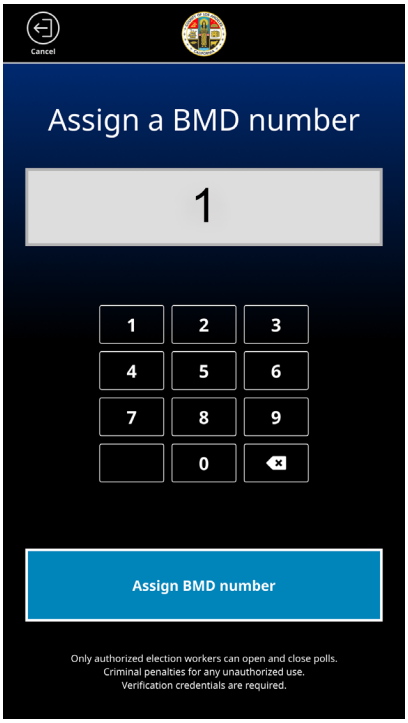
5. Tap **Open Polls**

Note: Screen displays a different **Poll Status** and **Total Ballots Cast** for the individual BMD if poll is opened more than once during the same election

Note: Ensure the **Voting Hardware** light is green and diplays **Passed Inspection**. This verifies the Printer (online/offline), Barcode Reader (online/offline), and memory available (at least 20% capacity). If light is red, power off the BMD and remove it from service.

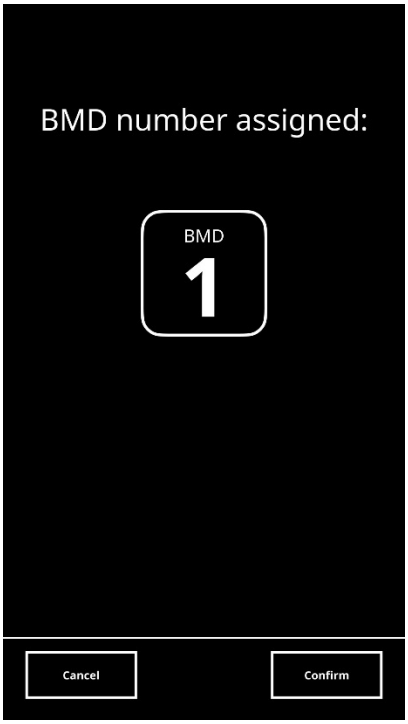


6. Assign a BMD number (unique for its vote center) to the BMD; press **Assign BMD number**

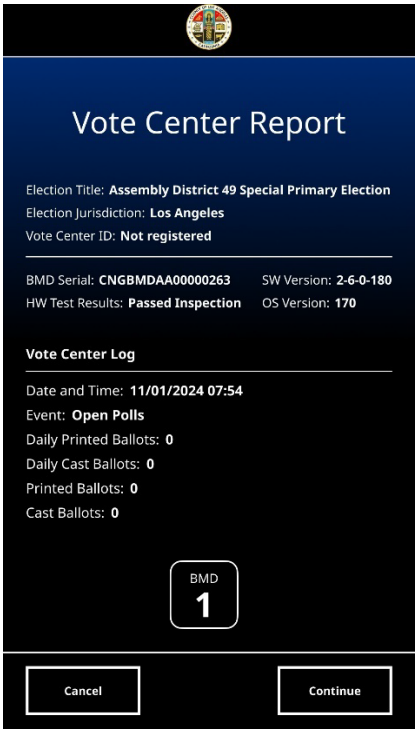


7. Click **Confirm**

Note: This number can be changed during an election and the confirmation instead appears as **Edit**

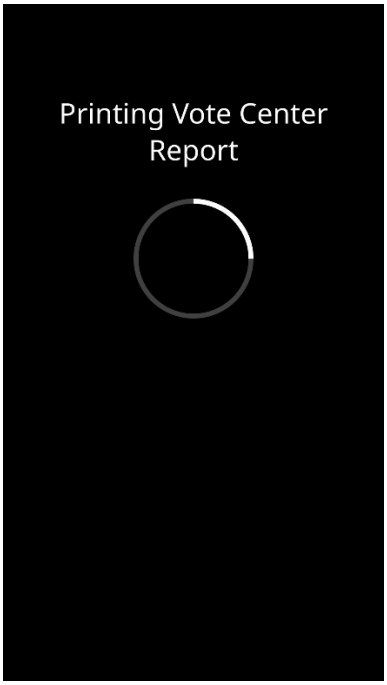


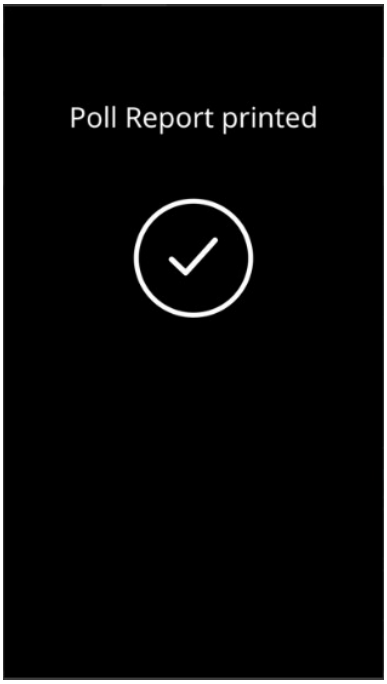
8. The Vote Center Report displays; tap **Continue**



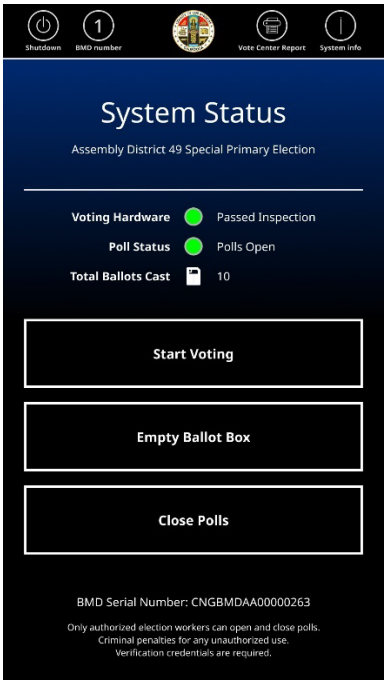
9. Insert **VSAP Report Paper** (or blank thermal paper) into the paper tray

Note: After the **Vote Center Report** is printed, Election Workers verify the report per LAC procedure

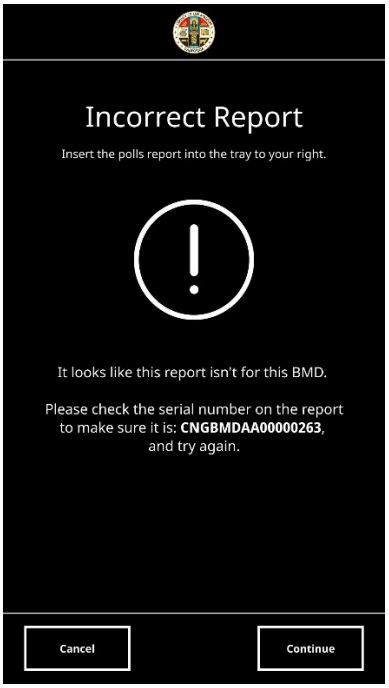


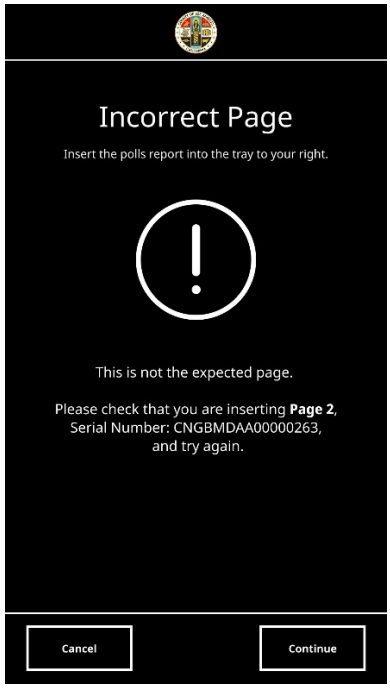


10. The **Poll Status** now displays **Polls** Open; tap **Start Voting** to enable voting

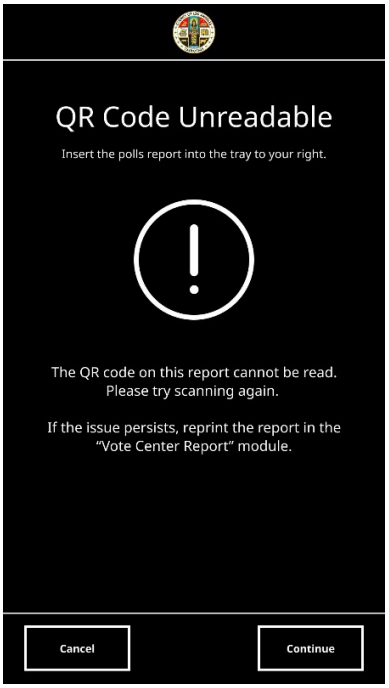


Note: Ensure the correct report is used for its corresponding BMD, as well as its correct page.

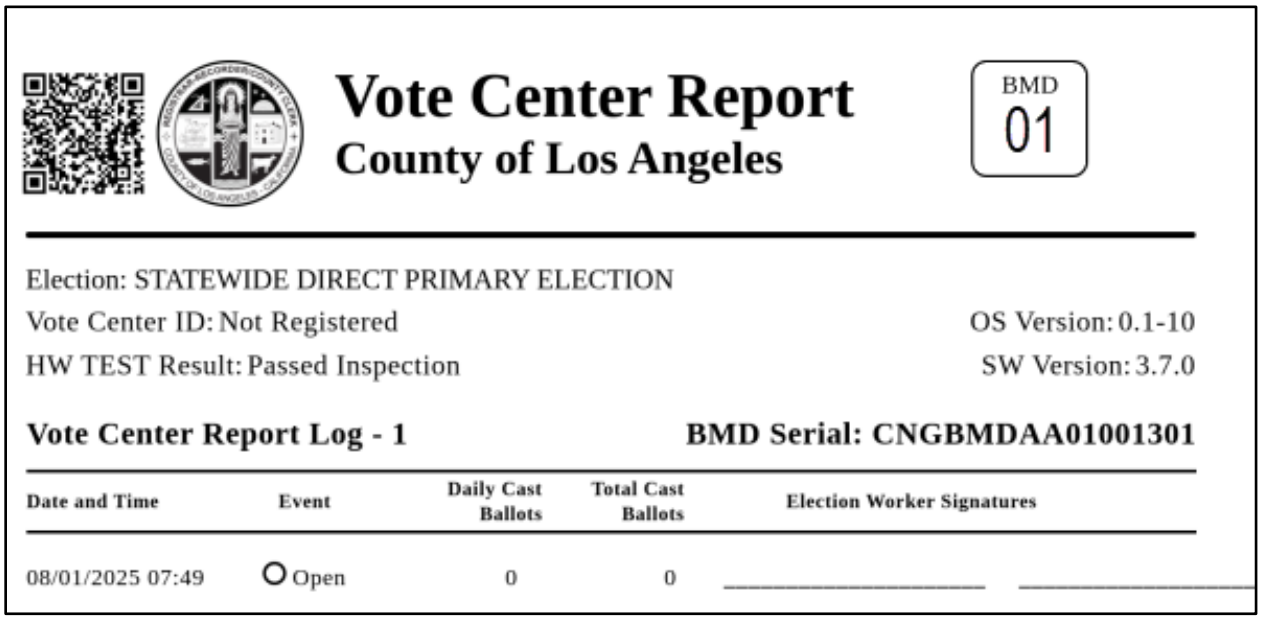




Note: If the QR Code cannot be read, reprint the report in the **Vote Center Report module**.



11.5.1. Sample Poll Report for the first day of an election



Vote Center Report
County of Los Angeles

BMD 01

Election: STATEWIDE DIRECT PRIMARY ELECTION
Vote Center ID: Not Registered
OS Version: 0.1-10
HW TEST Result: Passed Inspection
SW Version: 3.7.0

Vote Center Report Log - 1
BMD Serial: CNGBMDAA01001301

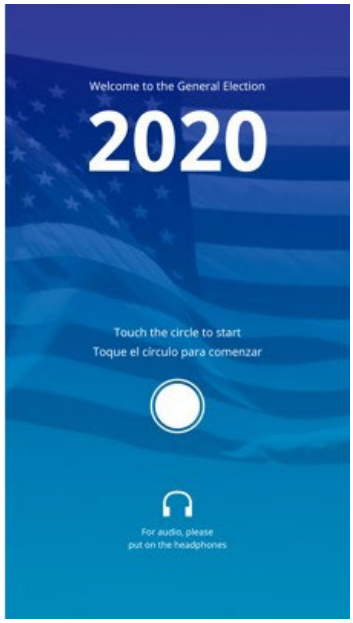
Date and Time	Event	Daily Cast Ballots	Total Cast Ballots	Election Worker Signatures
08/01/2025 07:49	O Open	0	0	_____ _____

11.6. Polling Procedures

11.6.1. Voting Using the BMD Touchscreen

An **Election Worker** provides the voter with an official paper ballot and directs them to any available **BMD**. The **BMD Touchscreen** displays a blue screen with the year and type of election (general or primary).

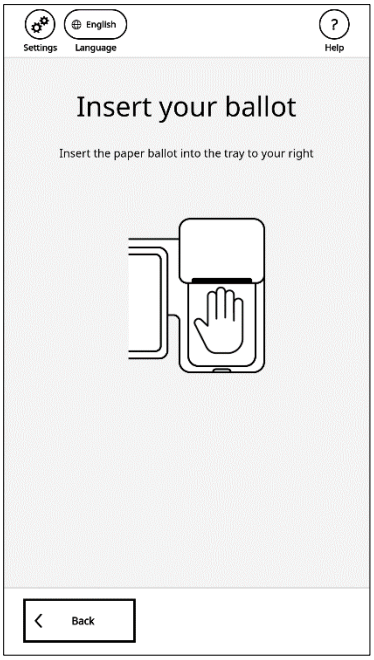
- Tap the **circle** to start



- Choose preferred **language**

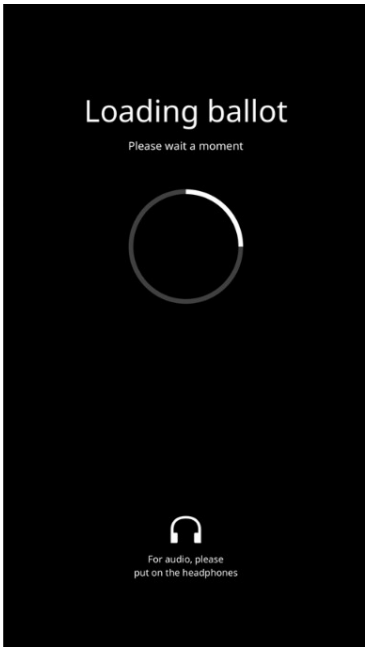
- Tap **Next**

System message: ***Insert your ballot***



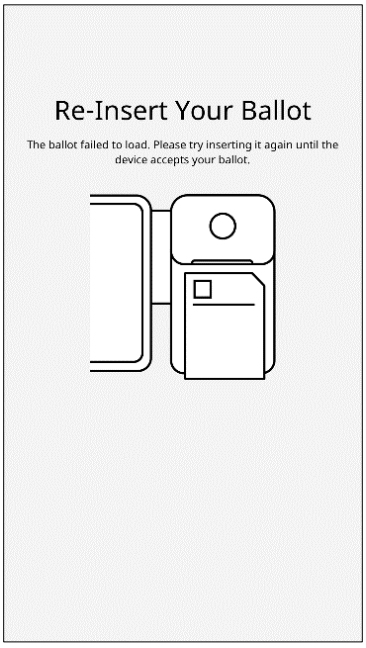
- Insert the **Ballot** into the paper tray on the right side of the ***BMD***

System message: **Loading ballot**

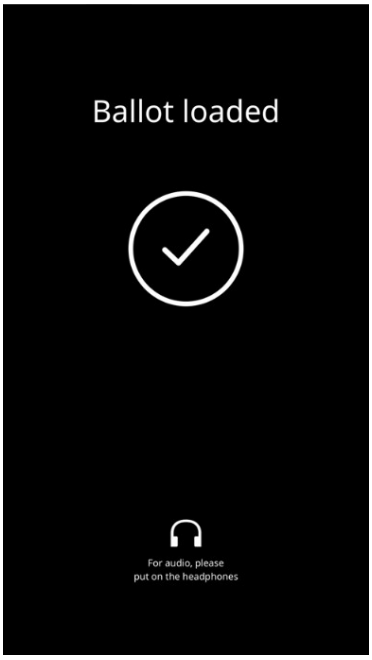


System Message: **Re-Insert Your Ballot** (appears when):

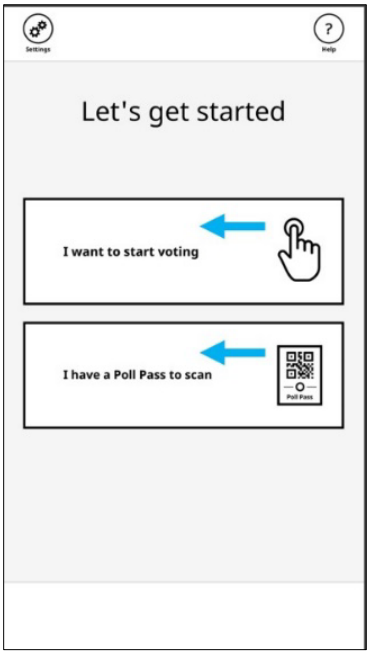
- Voter removed the ballot before it finished loading;
- Voter did not fully insert the ballot; OR
- Voter crookedly entered the ballot, so the system returned the ballot



System message: **Ballot Loaded**

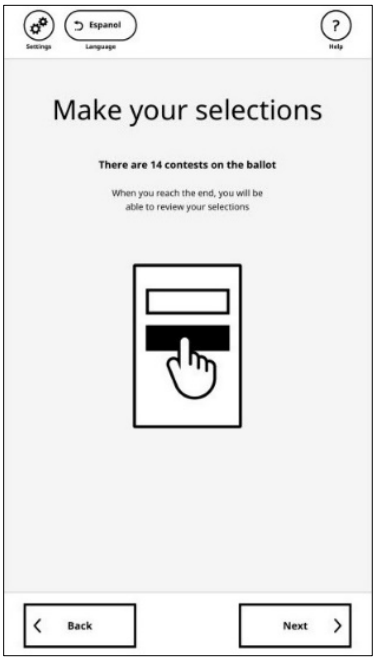


- The **Let's get started** screen displays two options; select one:
    - I want to start voting – Brings the voter to the Make your selections screen
    - I have a Poll Pass to scan – Asks the voter to Scan your Poll Pass



- Tap **Next**

System message: Make your selections



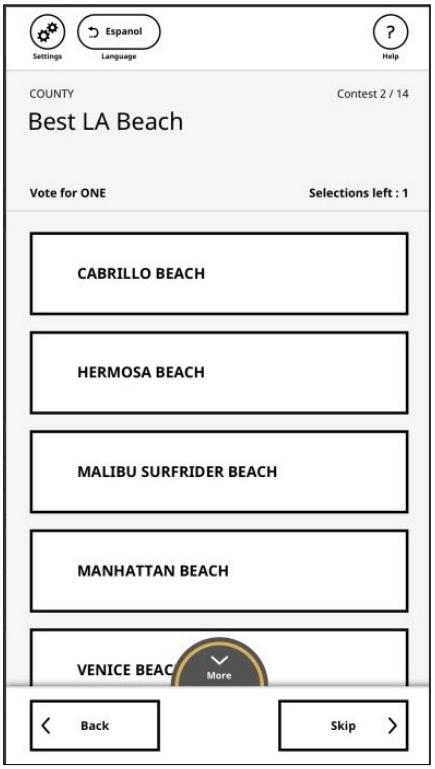
- Tap **Next** to begin voting

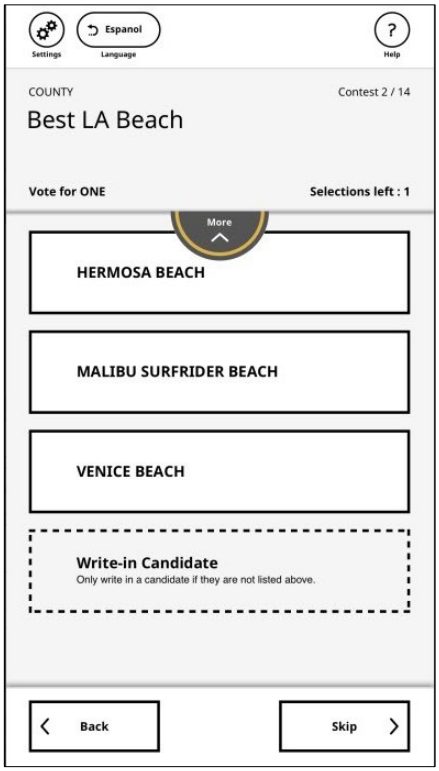
- Tap the **Candidate Name** or **Yes/No** for a **Proposition** or **Measure** to make a selection

- Tap **Next** to move to the next contest

- Marked selections are highlighted with a check mark
- To deselect, tap the marked selection – which will remove the highlighting and check mark
- To move past a contest without marking a selection, tap **Skip**

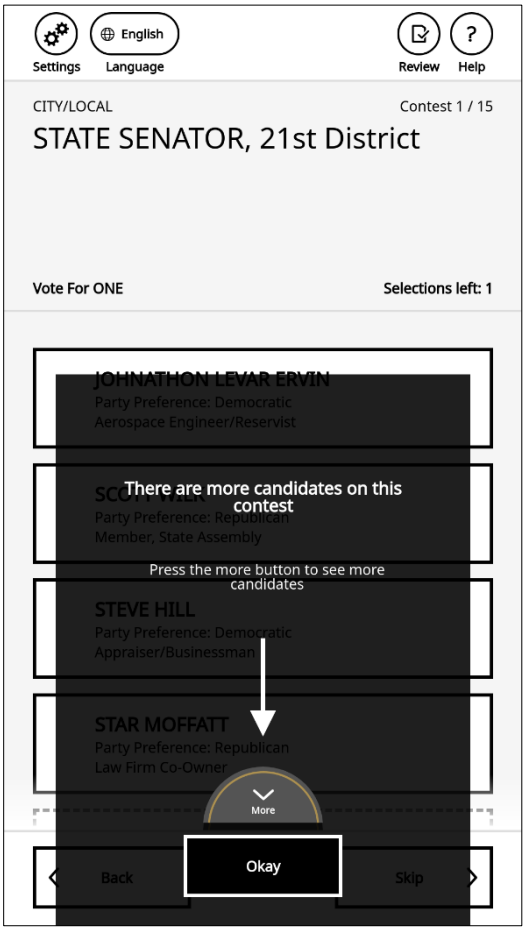
Sample contest





When the voter encounters any multi-page contest for the first time, a screen overlay with instructions for the **More** button appears:

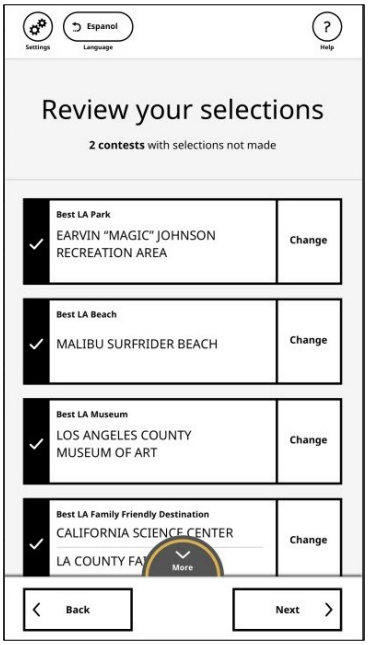
- The screen overlay explains there are more candidates on this contest; tap the **More** button to see more candidates
- The voter must tap **Okay** (or on any area of the BMD's Touchscreen) to clear the overlay before proceeding
- This screen overlay only appears once for each multi-page contest. The overlay will not display again on multi-page contests the voter has already viewed
- The **More** button is always visible on multi-page contests to navigate to additional candidates



System message: **Let's review**

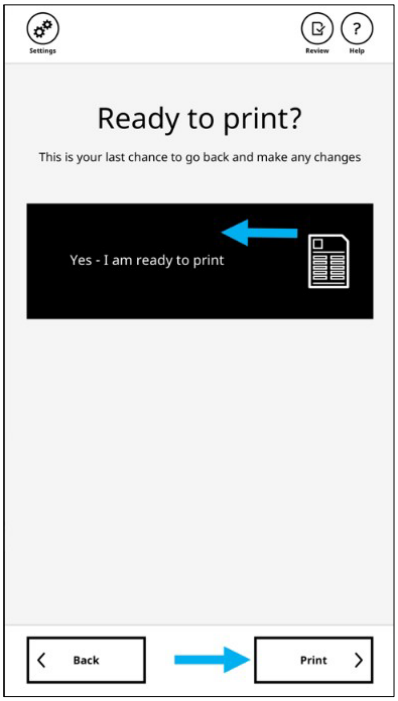
- Tap **Next**

System message: ***Review your selections*** (voters can tap the **Change** button to make a new selection)



- Tap **Next** when finished

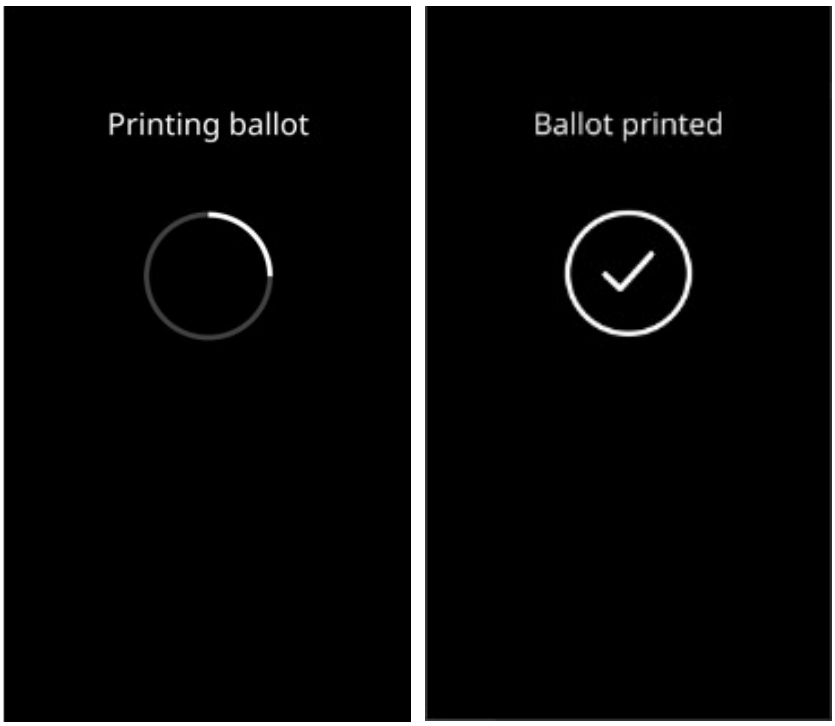
System message: **Ready to print**



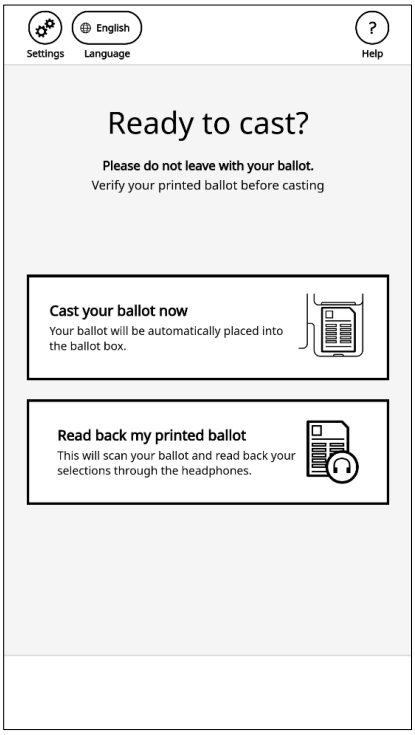
- Tap **Yes – I am ready to print**

- Tap **Print**

System messages: **Printing ballot** and **Ballot printed**



System message: **Ready to cast?**

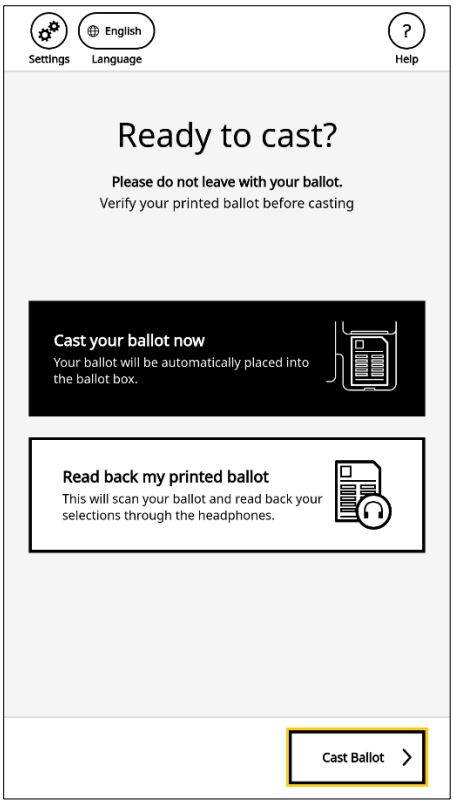


The voter can now do the following:

- **Cast your ballot now** – prepares the BMD to receive the voter's ballot
- **Read back my printed ballot** – rescans the ballot and reads back the voter's selections through the headphones
- Make a change on the printed ballot – the voter must contact an Election Worker; the Election Worker will spoil the ballot and provide the voter with a new ballot per County procedure

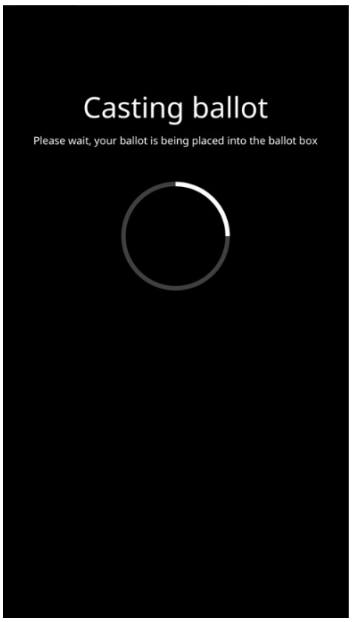
System message: Verify your printed ballot before casting

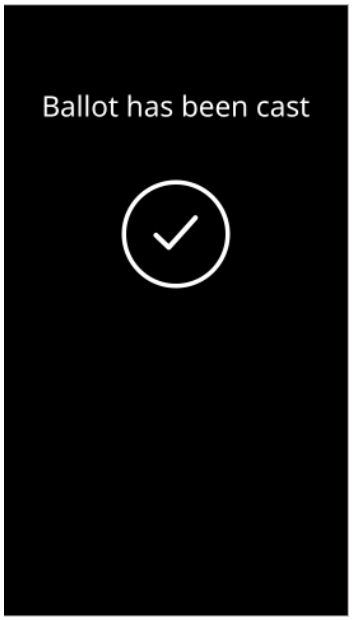
- Tap **Cast your ballot now**



System message: **Reinsert ballot to cast** reminds the voter to reinsert the ballot if removed from the BMD tray

System message: **Casting ballot** and **Ballot has been cast**

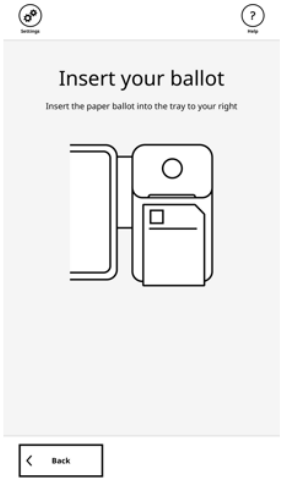




System message: **Thanks for voting!**

11.6.2. Using a Poll Pass

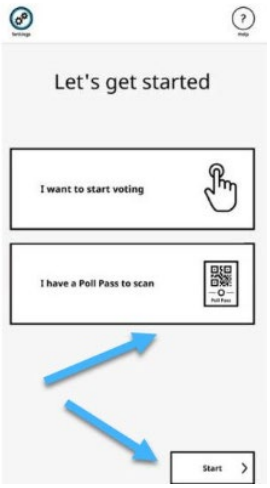
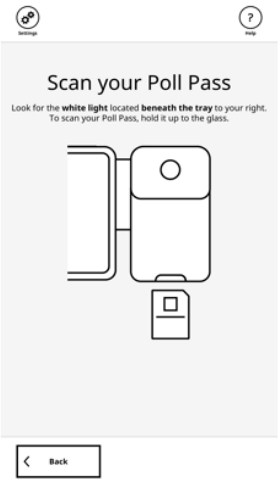
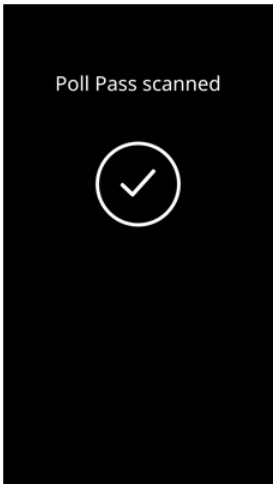
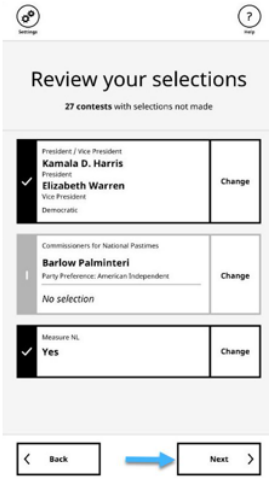
A voter can go online and access their sample ballot and digitally mark it using a computer or mobile device, such as a smart phone or tablet, prior to going to a Vote Center. Voter selections are captured in a QR code called a Poll Pass that can either be printed onto paper or downloaded to their mobile device. A sample of the Poll Pass is shown below. When the voter arrives at the Vote Center, they must check in using the normal check-in process.

1. Touch the circle to start the voting process	2. Tap a language	3. Insert ballot
		

Printed Poll Pass

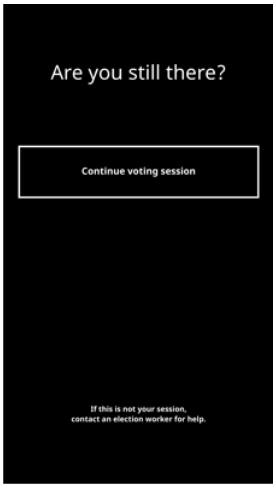
Mobile Device Poll Pass

After the voter has checked in and received a blank ballot, they will scan their Poll Pass at a BMD to transfer their selections to the BMD for validation before printing on a paper ballot.

4. After loading the blank ballot in the BMD, Ballot loaded is displayed	5. Tap I have a Poll Pass to scan and then click Start	6. Scan your Poll Pass screen will appear
		
7. Place your mobile Poll Pass or printed copy of a Poll Pass directly beneath the scanner located below the BMD paper deck	8. Message: Poll Pass scanned	9. Review and change selections as desired. Then tap Next
		

11.7. Dealing with Fleeing Voters

This procedure details what an Election Worker should do when a voter has left before casting their ballot.

1. If during a voting session, the voter stops interacting with the BMD for an administrator-specified period, the system will display the screen below. **Note:** If the voter has not fled, the voter can select Continue voting session	2. After a period of time (set by the BMG administrator), the BMD will lock out. The LED will flash yellow, indicating the BMD has timed out. At the bottom of the screen, the system will say: Notify an authorized election worker	3. The Election Worker will enter their Credentials and select Enter Poll Menu
		
4. The system automatically ejects the ballot and returns to the Welcome Screen. Follow LA County procedures to cast the ballot		

11.8. Voters with Disabilities and Voters Using Audio Features

This section describes procedures for voters utilizing the audio feedback, handheld controller, and customized screen settings.

11.8.1. Auxiliary Device and Ports

The BMD has two auxiliary ports, and one connected device which enables voters to mark and cast their ballots:

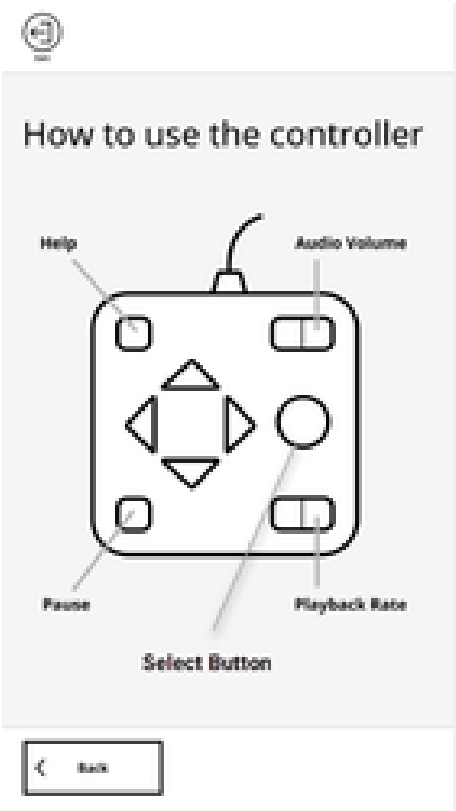
- Handheld Controller
- Headphones Jack
- Dual-Switch Port

11.8.2. Handheld Controller

The Handheld Controller allows the voter to use the BMD without having to touch the screen to navigate and mark their selections on the ballot. Braille is provided for voters with a visual impairment. The Handheld Controller has several components available for the voter, such as Help, Audio Volume, Pause,

and Playback Rate. There are also four directional arrow buttons used to navigate and a round button used to mark selections.

Handheld Controller



See table below for controller functionality:

Component/Location	Use/Functionality	Braille
Help	Press this button to access the help menu	Yes
Audio Volume	Press the audio button to increase or decrease the volume	Yes
Pause	Press the pause button to pause the voting process	Yes
Select Button	Press to select Candidate/Measure	No

Component/Location	Use/Functionality	Braille
Rate	Press the rate buttons to increase or decrease the rate of speed for listening to the ballot	Yes
Arrow Up	Press the arrow up to listen to the contest name above current candidate, Proposition/Measure	No
Arrow Down	Press the arrow down to listen to the contest name below the current candidate, Proposition/Measure	No
Arrow Right	Press the arrow to the right to make a selection to the right	No
Arrow Left	Press the arrow to the left to make a selection to the left	No

11.8.3. Headphone Ports

Headphones are located on the top left corner of the BMD and are plugged into the Headphones Jack located on the rear left-hand side, which automatically and continuously plays the audio voting instructions. There is an additional audio port provided at the left front of the BMD where a voter may plug in their own headphones. Both audio ports always remain active in case the voter desires a helper to listen to the voting session at the same time. The two audio ports are always at the same volume level and playback speed—changing the volume level or playback speed always affects both audio ports. The voter can plug in or unplug Headphones from either of the headphone jacks at any time, with no resulting message displayed by the BMD application. The audio can only be played in the language displayed on the screen.

11.8.4. Dual-Switch Port

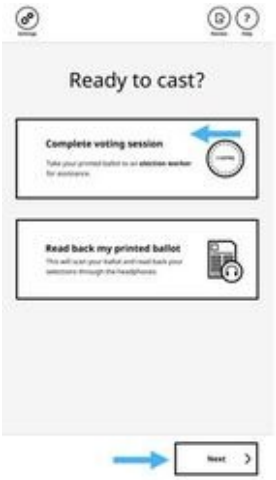
The right-front port is for connecting any dual-switch compatible device, such as a sip-and-puff assistive technology controller. The BMD application detects when a device is plugged into the port and shows a dual-switch specific configuration page that also informs the voter that if they are trying to plug in headphones, they should use the headphones jack. Audio will always be available when using the system regardless of what voting method is being used, i.e.: Touchscreen, Audio, or Poll Pass. The language displayed on the Touchscreen will be the same language used when using the audio voting feature.

11.9. Provisional Voters

This section details the procedure for assisting provisional voters. These voters receive a ballot containing a QR code indicating the vote is provisional. The voter's experience is the same with one exception - the voter cannot cast their ballot into the Integrated Ballot Box. Instead, they place their ballot in an envelope and return it to an Election Worker who will place the envelope in the Integrated Ballot Box per LA County procedure.

Note: The same procedure is used across precincts.

After marking their selections using the BMD, the voter will follow the steps below:

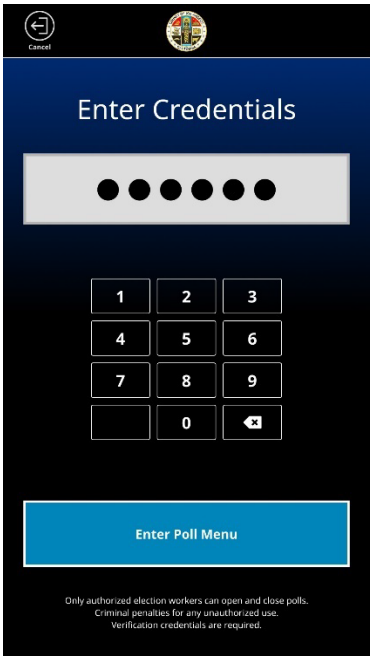
1. Tap Complete voting session on the Ready to cast? screen 2. Tap Next	3. Remove the provisional ballot and return it to an Election Worker	4. The screen displays Thanks for voting!
		

11.10. Closing the Polls and Vote Reporting

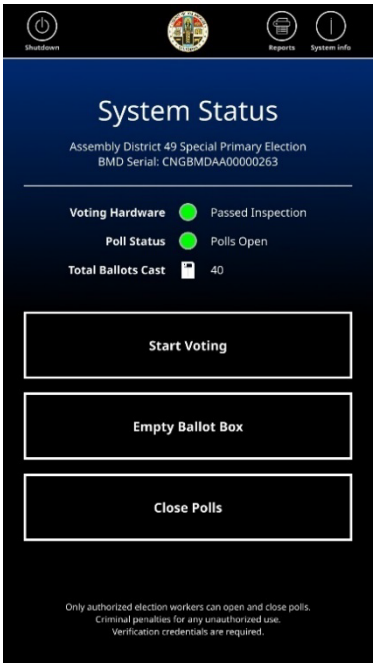
The following procedure must be used at each **BMD** to close the polls. The **Integrated Ballot Box** is emptied when closing the polls. After closing the polls, a final **Vote Center Report** is printed; this reports cumulative and daily totals for the **BMD**.

1. At the **Welcome/Idle** screen, scan the Security pass under the right-side of the BMD

2. Enter the six-digit PIN; tap **Enter Poll Menu**

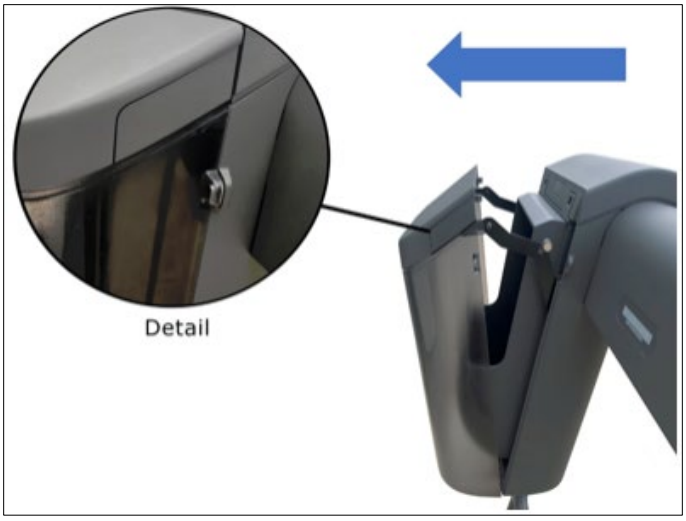


3. Tap **Close Polls**

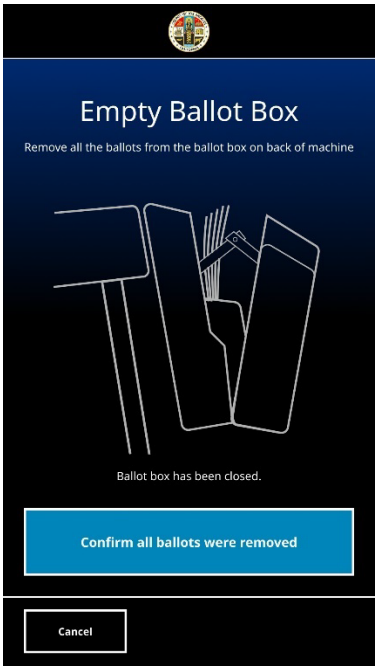


4. The **Empty Ballot Box** prompt displays; remove the zip tie and tamper-evident seal on the seam of the Integrated Ballot Box; record the removal in the Chain of Custody per LA County procedure

5. Open the **Integrated Ballot Box** by pushing the button on the upper-left side of the **Ballot Box**, then pulling the back outward

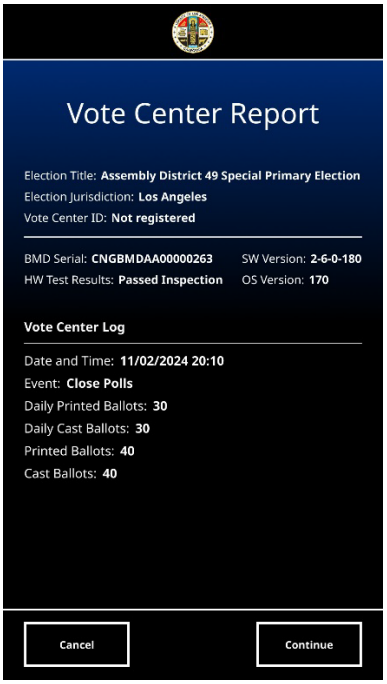


6. Remove all ballots and tap **Confirm all ballots were removed**



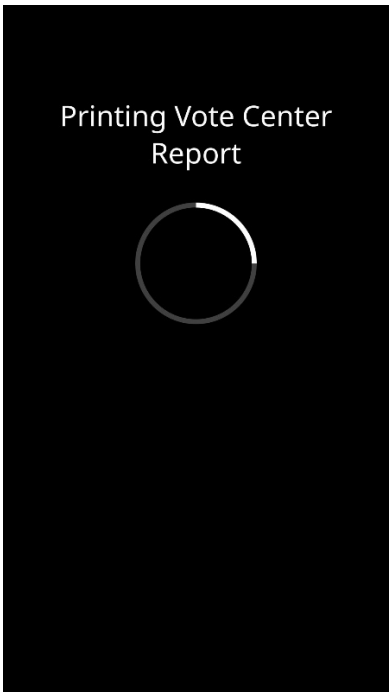
7. Close the **Integrated Ballot Box** until it clicks to ensure it is properly closed

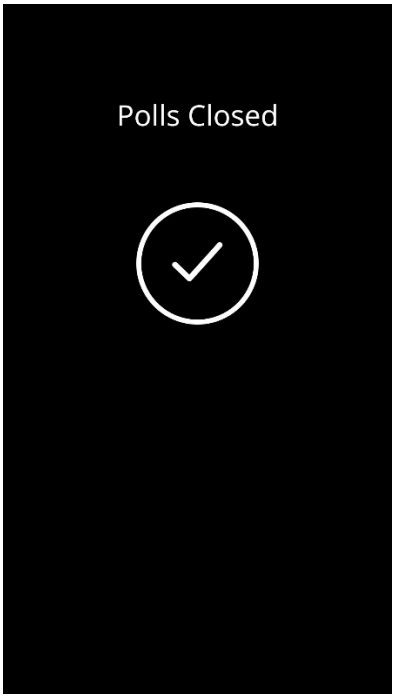
8. The **Vote Center Report** displays; click **Continue**



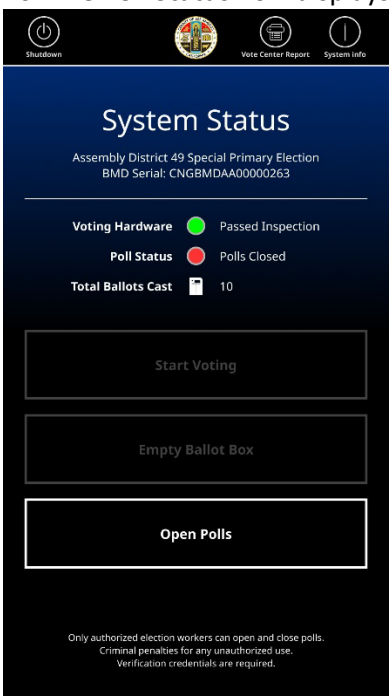
9. Insert **VSAP Report Paper** (or blank thermal paper) into the paper tray

Note: After the **Close Poll Report** is printed, the report must be signed and reconciled by Election Workers per LAC procedure





10. The **Poll Status** now displays **Polls Closed**; tap **Shutdown** to disable voting



Close Poll Report

Sample Poll Report for re-opening and closing the poll throughout an election:

Vote Center Report
County of Los Angeles

BMD 01

Election: STATEWIDE DIRECT PRIMARY ELECTION
Vote Center ID: Not Registered
HW TEST Result: Passed Inspection
OS Version: 0.1-10
SW Version: 3.7.0

Vote Center Report Log - 1 **BMD Serial: CNGBMDAA01001301**

Date and Time	Event	Daily Cast Ballots	Total Cast Ballots	Election Worker Signatures	
08/01/2025 07:49	○ Open	0	0	_____	_____
08/01/2025 18:00	● Close	25	25	_____	_____
08/02/2025 08:00	○ Open	0	25	_____	_____
08/02/2025 18:30	● Close	20	45	_____	_____
08/03/2025 09:00	○ Open	0	45	_____	_____
08/03/2025 17:00	● Close	10	55	_____	_____
08/04/2025 08:30	○ Open	0	55	_____	_____
08/04/2025 19:30	● Close	15	70	_____	_____
08/05/2025 07:00	○ Open	0	70	_____	_____
08/05/2025 18:10	● Close	50	120	_____	_____
08/06/2025 08:20	○ Open	0	120	_____	_____
08/06/2025 18:20	● Close	5	125	_____	_____
08/07/2025 08:20	○ Open	0	125	_____	_____
08/07/2025 16:24	● Close	30	155	_____	_____
08/08/2025 08:00	○ Open	0	155	_____	_____
08/08/2025 19:23	● Close	10	165	_____	_____
08/09/2025 08:11	○ Open	0	165	_____	_____
08/09/2025 18:03	● Close	20	185	_____	_____
08/10/2025 07:20	○ Open	0	185	_____	_____
08/10/2025 16:24	● Close	0	185	_____	_____
08/11/2025 08:00	○ Open	0	185	_____	_____
08/11/2025 19:11	● Close	65	250	_____	_____

End of Page

Note: This final Vote Center Report must be signed by two election workers and reconciled per jurisdictional procedure.

11.11. Securing Audit Logs and Backup Records

See Section 19. Audit Trails for further details.

11.12. Troubleshooting and Problem Resolution

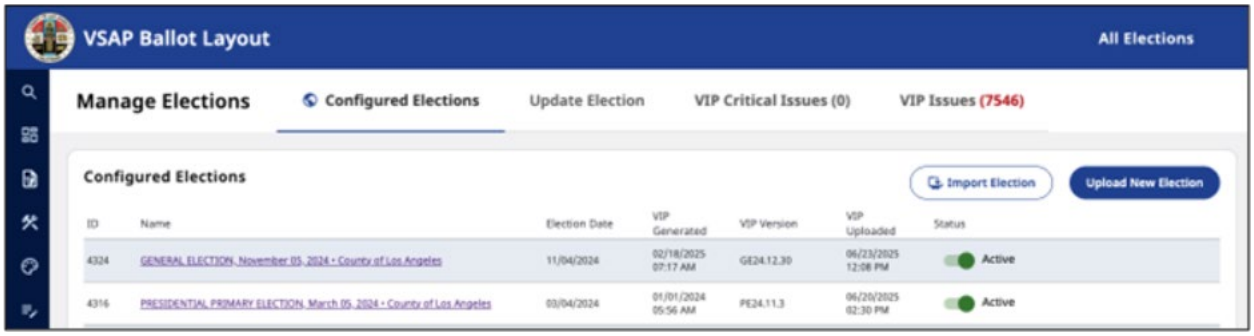
Problem	Solution
Frozen BMD Touchscreen • Frozen on any screen in the voter's workflow • Black (white) screen displays	If the Touchscreen froze due to voter interaction (such as inserting a Ballot with a faded or out of position BPM QR Code): 1. Retrieve the voter's Ballot and move the voter to another BMD 2. Power off the BMD 3. Turn back on 4. If the error did not clear out, remove from service If the Touchscreen froze for any other reason: 1. Power off 2. Remove from service 3. Mention in Help Desk Ticket that the "image may need to be taken"
BMD cannot read a Ballot with the voter's printed selections - after it has been reinserted into the BMD	1. Insert the Ballot into another BMD 2. If the second BMD is unable to read the Ballot, cast the Ballot into a general Ballot Box
Headphones are not working	1. Check headphones are plugged into an audio port 2. Plug headphones into the other audio port and try again 3. Replace headphones and try a new pair of headphones 4. Move the voter to another BMD and remove the BMD from service
Dual Switch is not working	1. Ensure the dual-switch is plugged in 2. Take the voter back to one of these points in the voter's workflow: a. Welcome/Idle screen b. Screen right after Ballot has been inserted c. Language selection screen 3. Try the dual-switch on another BMD 4. If it works on the other BMD, remove the first BMD from service **Note**: Dual-switch can only be activated at these three points in the voter's workflow

Handheld Controller is not working	1. Verify the "**Audio with Controller"** setting is selected 2. If the Controller still does not work: 3. Move voter to another BMD 4. Remove the BMD from service
Paper jam – Ballot jams while ejecting / scanning Ballot	1. Clear the paper jam and cancel voting session 2. Spoil the Ballot 3. Issue the voter a new Ballot
Paper jam – Ballot jams while printing	1. Clear the paper jam 2. Spoil original Ballot 3. Reprint Ballot 4. Cast reprinted Ballot
Paper jam – Ballot jams while casting	1. Remove the jammed Ballot 2. Give the voter an "I Voted" sticker 3. If the Ballot is not damaged, reinsert and cast into the BMD 4. If the Ballot is damaged, send to the Check-in Clerks to remake the Ballot
Paper jam screen is shown while printing the Open/Close Poll Report	1. Remove jammed Poll Report 2. Insert new VSAP Report Paper to reprint the Poll Report

12. Ballot Layout Procedures

The foundational step a VSAP Ballot Layout user must take in setting up an election occurs on this page, where they can load in election data. Election data is provided by the County candidate filing system as a VIP file (VIP, a format from the Voting Information Project, refers to the data structure chosen for this ingestion).

VIP files are uploaded to VBL, and precede the configuration of VBM ballots, BMD ballots, and generating election files. This is where users can also view VIP file issues that may block configuration combinations or generating ballots or files. VIP Issues are organized in a way to guide users in resolving problems within VBL or in the VIP file data itself.



12.1. Configured Elections

This tab displays All Elections set up in VBL, both active and inactive. It also displays the current VIP defining each election. The listed elections serve as quick links, directing the user to those election Dashboards.

To set up a new election:

- Click on Upload New Election
- Choose File from your computer
- Click on Save and Upload
- The VIP begins processing in VBL. Users gain access to the election after several seconds, but the full saving and setup of the election takes several minutes. During this time users will have limited access to the following functionality:
    - Assign Party Tints
    - Alter VBM Ballot Configuration
    - Alter BMD Ballot Configuration
- “An election is currently being uploaded. Please wait for upload to finish.” will display as a banner on any of the election specific pages while the election is setting up.
- If the VIP upload fails, the banner will display this failure throughout the application.
- If the VIP upload succeeds, a green banner will appear temporarily and the VIP information will update to reflect the newly uploaded VIP.

Vote By Mail is where the user conducts the configuration and generation of various ballot layout combinations across languages to produce ballots, supersets to streamline proofing, and split PDFs for eventual printing and distribution.

12.2. VBM Configuration

The VBL system allows users to configure the Vote-By-Mail ballots to optimize the layout and fit all contests in an upcoming election.

Configure VBM ballots:

- Navigate to the VBM Configuration page under Vote by Mail from the menu drawer.
- The General VBM Configuration table displays the current configuration.
- Click Edit icon to edit the configuration, selecting from the following in the Edit General VBM Configuration modal:
    - Paper Size. Size of the paper ballot and the number of times to fold it to fit in the envelope.
    - Letter
    - Legal
    - Ledger
    - Monolingual or Bilingual Ballot:
        - Monolingual. Non-English ballots will not display English translations but will print both the English and translated versions of candidate names.
        - Bilingual. Non-English ballots will include English translations of all ballot content.
    - Key Card Anchor. Select which card in each ballot packet is designated to be the Key Card when scanned in Tally.
        - First Card
        - Last Card
        - Contest(s): One or many contests in an election can be selected and the card with that contest in each ballot packet will be the Key Card. In the case that multiple contests are selected and more than one of the selected contests are in the same packet, the first contest in the list will be designated as the Key Card contest.
- Click Save Configuration
- Click the Edit button in the VBM Configuration by Language able to edit the desired row's configuration, selecting from the following in the Edit VBM Configuration modal:
    - Columns – Number of columns on each page of the ballot:

        - 2-column (letter and legal paper only)
        - 3-column
        - 4-column (ledger paper only)
    - Compression & Fitting:
    - Reduce Line Wrapping: The forced line break between the candidate party preference and candidate occupation is removed and replaced by a comma and space character. This rule affects all contests except the presidential contest.
    - Compressed Layout: The default padding around all content on the ballots is reduced by 10 percent and some content font size is reduced to 8pt. This setting can be used to reduce how much space a contest takes on a page to reduce paper usage for ballots. These are the default settings for compressed layout and may be changed by an administrator through the layout_config.json.
    - Start the first contest on the second column of the ballot
    - Suppress contest headings if division and contest headings match.
- Click the Add a Language Configuration button to add a language specific configuration.

12.3. Generate Ballots

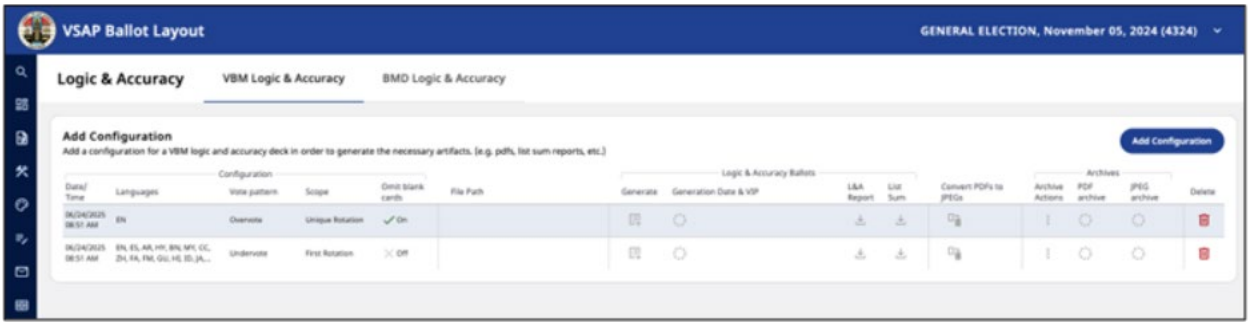
Once election managers have optimized layouts for Vote by Mail (VBM) ballots they generate the ballots which applies the configurations and layout rules to the election data appropriately.

Generate ballots:

- Navigate to the Generate Ballots page in the menu drawer under the Vote by Mail heading.
- The default tab, the Generate Ballots tab contains primary VBM ballot functions such as Ballot Preview, Generate Ballots, Current VBM Configuration, and Ballot Generation History.
- Configure the generation in the Generate VBM Ballots card.
    - Language Configuration: Select one or more languages to run in a VBM generation.
    - Party Configuration: Will display if a partial is selected to be generated. Select one or more parties to have ballots generated during the next run of VBM generation.
    - Layout or Contests configuration: Will only display if a partial is selected to be generated. There are three options to choose from.
    - All: All ballot styles will be generated.
        - Contest Selection. Select one or more contests from the election.
        - Layout Selection. Select an individual or a range of ballot layouts to be generated.
- Start VBM generation by clicking Generate Ballots. Important: Generation can take several hours depending on the size of the election.

12.4. Logic and Accuracy

Logic & Accuracy decks allow for appropriate testing scenarios of downstream VSAP systems. The user can generate a Logic and Accuracy deck based on set configurations and create archives of generated L&A decks so they can be retrieved for the appropriate testing.



Configure VBM L&A ballots:

Navigate to the VBM Logic & Accuracy page under Logic & Accuracy from the menu drawer.

- Click Add Configuration at the top right of the page and select from the following options:
  - Language Configuration:
  - Scope of Contests to Vote.
  - First Rotation
  - Unique Rotation
  - Reporting Unit
  - Ballot Layout
  - Omit Blank Cards.
  - Choose whether to include or omit pages that contain no contests.
  - Vote Patterns By Candidate
  - Configure how the predetermined votes on the L&A deck should be patterned
  - Undervote
  - Overvote
  - Ascending
  - Patterned (Enter the desired vote-for pattern in the text box, separating each number with a comma)
  - Random (Enter the desired Minimum and Maximum (cannot exceed 50) number of votes per candidate)
- Save the new configuration by clicking Add Configuration.
- A new row will be added to the Add Configuration table below. The table is sorted by latest to oldest generation. Users will be able to see:
  - Date/ Time. Displays when the configuration was added
  - Languages. Languages supported for this configuration
  - Vote pattern
  - Scope
  - Omit blank cards
  - File Path
  - Logic & Accuracy Ballots
- To create test ballots, click the Generate button; the following information will appear with new actions:
  - Generation Date & VIP. While generating will display the Cancel Generation button. After generation will display when the configuration was generated.
  - L&A Report download button
  - List Sum download button
  - Convert PDFs to JPEGs
  - Archives
  - Archive Actions. Button to create the PDF and JPEG archives

- PDF archive
- JPEG archive
- Delete

Configure a BMD L&A:

- Navigate to the BMD Logic & Accuracy page under Logic and Accuracy from the menu drawer.
- Click Add Configuration and make the following selections:
    - Scope of Contests to Vote
    - Vote Patterns (Configure how the predetermined votes on the L&A deck should be patterned)
- Save the new configuration by clicking Add Configuration.
    - A new row in the BMD Logic & Accuracy table below will be added.
- Navigate to the BMD Logic & Accuracy page under Logic and Accuracy from the menu drawer.
- Click the icon under the Generate column to begin generation for the desired BMD L&A configuration.

12.5. Election Files

Election files are used to configure downstream VSAP systems (Tally, BMG, BMD, etc.) to operate appropriately for an upcoming election.

Download Election Files:

- Navigate to Election Files under Download Files in the menu drawer.
- Click the Download icon to the right of the file name, size, and version.
    - If the file is not ready for download, the download icon will be disabled and the Notes column will say which processes need to be run.
- To download all the election configuration files as a single zip (excluding the EAP) click Download All at the top right of the Election Files.

Download Election Audio Package (EAP):

Requires EAP Validation to run before this file can be downloaded. This file can be downloaded even if the audio package fails validation (the Notes column will say EAP is incomplete).

- Click the download icon to the right of the file name, size, and version to download the EAP as a single zip.
    - If no EAP has been uploaded, the download icon will be disabled.

12.6. Tally Procedures

Ballot scanning may be conducted prior to election night as part of the preparation process. This step is essential to capture ballot images in advance, ensuring they are ready for tabulation once results reporting begins on election night.

At least one election needs to be configured before a user can access the rest of Tally Manager. Selecting **New Election** opens the modal to set up an election.

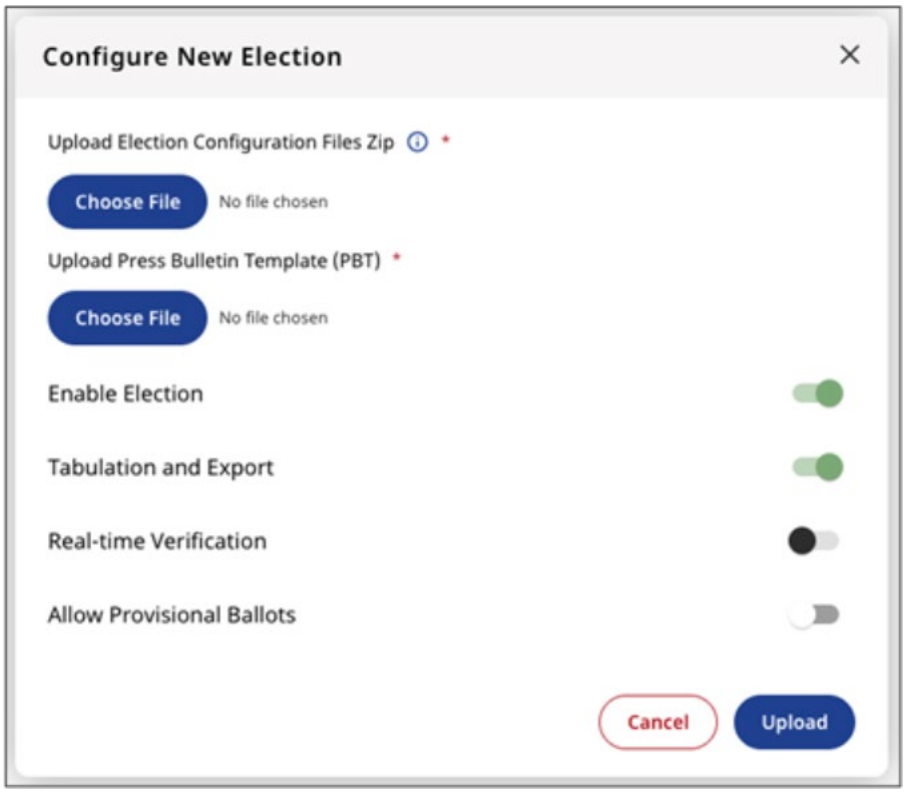


Figure: *Configure (set up) a new election*

To configure a new election, 2 files are now required:

- Election Configuration Files .ZIP
- PBT - Press Bulletin Template

The BDF, TLDF and DMF are election configuration files that are generated by VSAP Ballot Layout (VBL) and combined in a single Election Configuration File .ZIP. The zip file from VBL also contains some other files that, while not used by Tally, may be left in the file uploaded to Tally. The PBT is generated by the Election Contest and Ballot Management System (ECBMS) when the Voting Information Project (VIP) file is created. The PBT is uploaded as a text file and the Election Configuration Files .ZIP is uploaded as a .ZIP file.

In addition to uploading the necessary files, there is the option to set:

- Enable Election
  - ON means it is an active election
  - OFF means the election is disabled
- Tabulation and Export
  - ON means production data can be tabulated and that an Export and/or CVR report can be generated.
  - OFF means only test data can be tabulated and users cannot generate an Export or CVR Report.
- Real-time verification
  - ON means the Verify service will validate the signature of Ballot Marking Device (BMD) ballots as Tally processes ballots.

  - OFF means the Verify service will not validate the signature of BMD ballots and tag the verify status as pending.
- Provisional Ballots
  - ON means provisional ballots will be allowed by the Refine service and not outstacked.
  - OFF means provisional ballots will not be allowed by the Refine service and will be outstacked.

The Ballot processing card gives the operator an overview of how the system is functioning including the number of services of each time that are running and the collective throughput of each kind of service.

This provides the operator with an understanding of the rate the room is running as well as a first indication of potential system issues or bottlenecks. Under normal operation, the expectation is that the numbers across each service type basically match - although small variations over time are expected.

This card also provides the outstacks from each service type in the last minute, the current day, and the entire election giving the operator a sense of current trends and if outstack rate are unexpectedly high.

Clicking a service link in the service column opens the Ballot Processing page and navigates the user to the corresponding service tab.

Clicking on the Ballot Processing title in the dashboard card navigates users to the Ballot Processing page in Tally, which defaults to the Scanners tab.

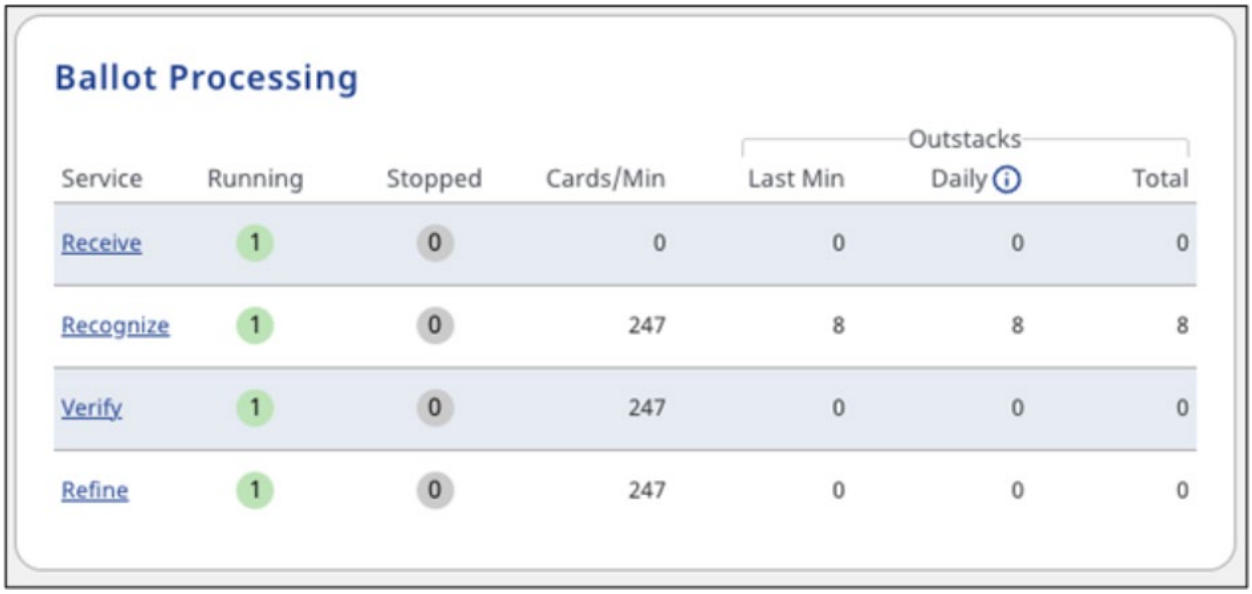
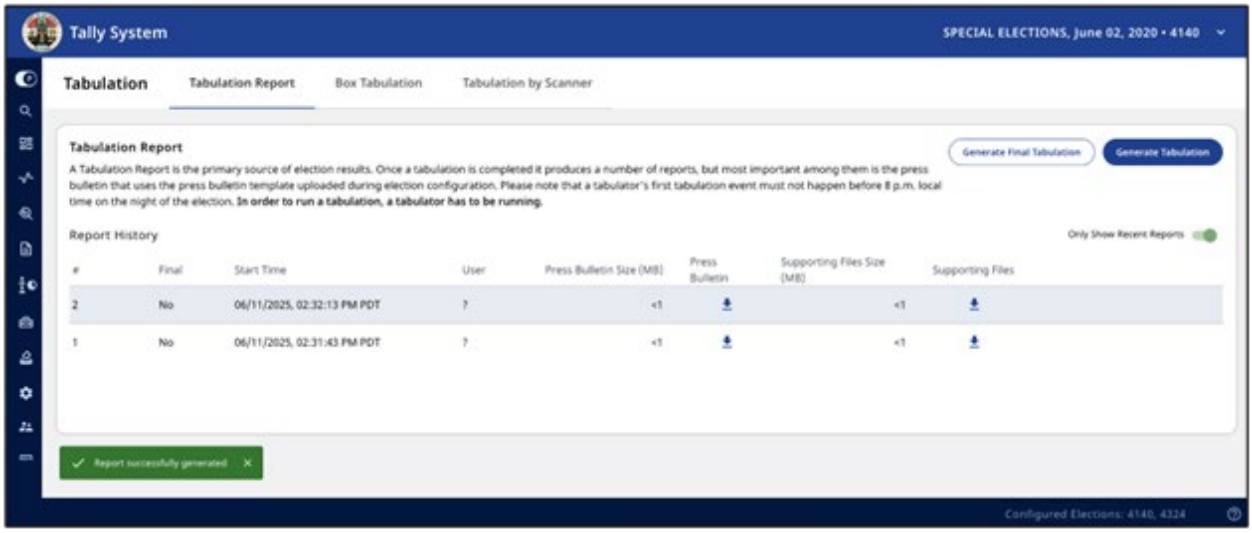


Figure: *Ballot Processing dashboard card*

After all the ballots have been processed by Receive, Recognize, Verify, and Refine, the user can generate and view reports. Using the navigation sidebar navigate to Tabulation > Tabulation Report. A tabulator's first tabulation event must not happen before 8 p.m. local time on the night of the election. This is fully managed through the election process.



12.6.1. Generate Report

1. From the heading drop-down, select the election that needs reports run
2. Set the test/production toggle to match the type of ballots processed
3. Refresh the page
4. Select the type of report needed -- Tabulation Report (overall), Box Tabulation, or by Scanner
5. For Tabulation Report, click the “Generate Tabulation” button, and after a short time a new Press Bulletin link will be generated along with supporting downloadable files. Click on the Press Bulletin link and review the Semi-Final Election results that display in a new browser tab

12.6.2. Generate Final Report

1. Select the type of report needed and click on the “Generate Final Tabulation” button. After a short time, a new Press Bulletin link will be generated with a “Yes” in the Final column
2. Click on the Press Bulletin link and review the Final Election results that display in a new browser tab

12.7. Shutdown Procedures

Shutting down services stops all services that are not needed to provide basic UI functionality, this includes all active instances of receivers, recognizers, verifiers, refiners, tabulators, ballot viewer, marksense, card tracker, and outstacker. The services will also be scaled down to 0, so they are not automatically restarted by Kubernetes.

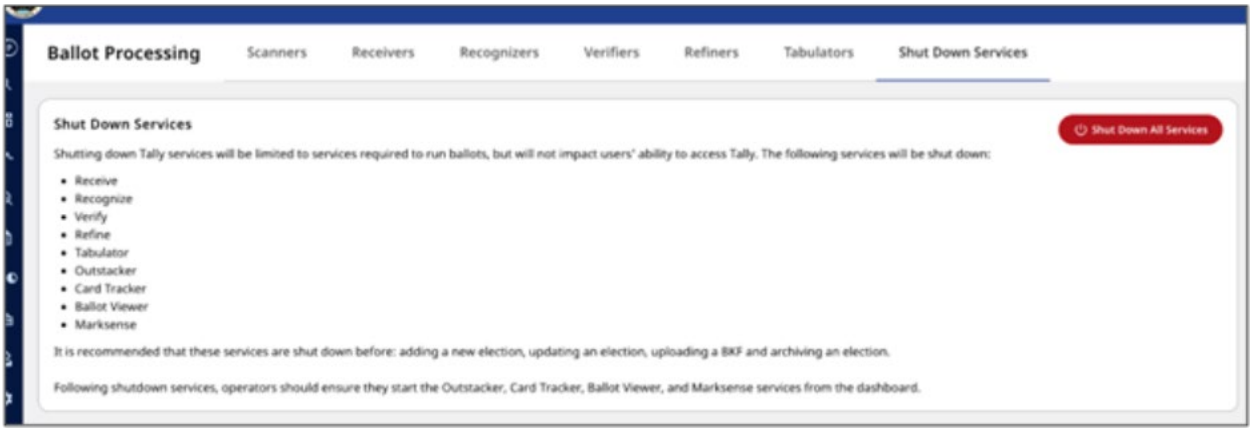


Figure: *Shut down services page*

VoteCal Candidate Filing and Election Night Reporting (CFENR) Module

Officials comply with election night vote reporting by using electronic files. These reports are uploaded to the Secretary of State CFENR system via sftp. The CFENR system retrieves the report, transfers the data to the database, and processes the information into the Secretary of State elections reporting system.

When the red **Shutdown Services** button is clicked, a modal displays to let the administrator confirm that the services should be shut down.

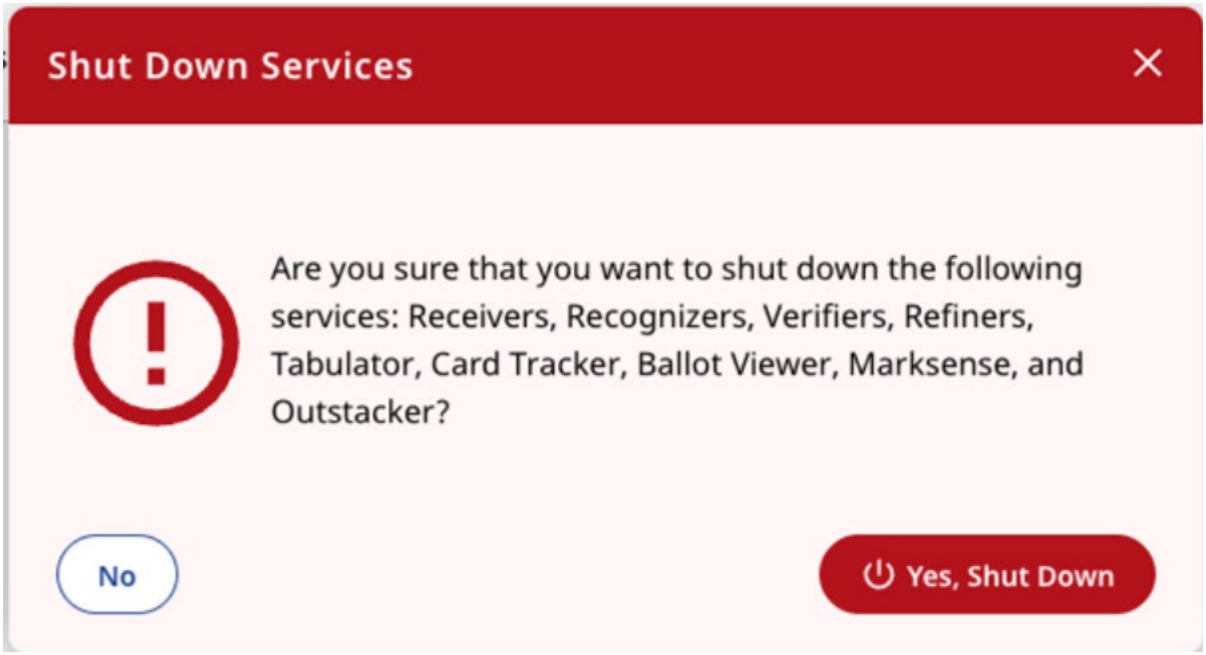


Figure: *Shutdown Services confirmation modal*

After the services have been shut down manually, they can be restarted from the dashboard.

13. Semi-Official Canvass, Official Canvass, and Post-Election Procedures

13.1. Election Observer Panel

The purpose of Election Observers is to:

- Provide an avenue for public observation of and input into the election process
- Assist in ensuring the integrity of the election process
- Encourage participation and build voter confidence in the election process

13.1.1. Invitation

Between E-60 and E-30, prepare a media release and letters of invitation (see samples attached) to parties likely to participate, such as the following:

- County Grand Jury
- Political Party Central Committee Members
- Language Advocacy Groups
- Community Based Organizations
- Media

Other groups or individuals expressing an interest in observing election day activities may also be included in the observer panel, as deemed appropriate.

13.1.2. Mechanism for Feedback

Observers attend training at government facilities, where they can ask questions about the process.

13.1.3. General Rules for Observers

Election Observers have the right to observe voting and election-related processes. Moreover, Election Observers have the right to challenge election-related processes. They also have the right to submit written challenges for review at a later time. These written challenges will be documented and resolved as provided in Section 20879(h). Upon the resolution of a challenge, the County shall provide the Election Observer with an oral or written disposition of the challenge as soon as is reasonably practicable. The County must ensure that no confidential voter registration information is disclosed when providing the disposition of the challenge. For more information, an Election Observer Panel Plan is available upon request.

13.2. Canvassing Precinct Returns

13.2.1. Time for Conducting Canvass

The canvass shall commence no later than the Thursday following the election, shall be open to the public, and, for state or statewide elections, shall result in a report of results to the Secretary of State. The canvass shall be continued daily, Saturdays, Sundays, and holidays excepted, for not less than six hours each day until completed.

13.2.2. Tasks of the Official Canvass

The official canvass shall include, but not be limited to, the following tasks:

- An inspection of all materials and supplies returned by poll workers
- Processing and counting any valid vote-by-mail and provisional ballots not included in the semifinal official canvass
- Counting any valid write-in votes
- Reproducing any damaged ballots, if necessary
- Reporting final results to the governing board and the Secretary of State, as required

13.3. Canvassing Vote by Mail Ballots

13.3.1. Processing and Counting Vote by Mail Ballots

Vote-by-mail ballots and mail ballot precinct ballots returned to the elections office and to the polls on or before election day that are not included in the semifinal official canvass phase of the election, including any ballots returned to another jurisdiction in the state and forwarded to the elections official who issued the ballot, shall be processed and counted during the official canvass as described below.

“READ THESE INSTRUCTIONS CAREFULLY. FAILURE TO FOLLOW THESE INSTRUCTIONS MAY CAUSE YOUR VOTE BY MAIL BALLOT NOT TO COUNT.
1. We have determined that the signature you provided on your vote-by-mail ballot does not match the signature(s) on file in your voter record. In order to ensure that your vote-by-mail ballot will be counted, the signature verification statement must be completed and returned as soon as possible.

2. The signature verification statement must be received by the elections official of the county where you are registered to vote no later than 5 p.m. two days prior to certification of the election.
3. You must sign your name where specified on the signature verification statement (Voter's Signature).
4. Place the signature verification statement into a mailing envelope addressed to your local elections official. Mail, deliver, or have the completed statement delivered to the elections official. Be sure there is sufficient postage if mailed and that the address of the elections official is correct.
5. If you do not wish to send the signature verification statement by mail or have it delivered, you may submit your completed statement by email or facsimile transmission to your local elections official using the information provided."

"SIGNATURE VERIFICATION STATEMENT
I,, am a registered voter of _____ County,
State of California. I declare under penalty of perjury that I requested and returned a vote-by-mail ballot. I am a resident of the precinct in which I have voted, and I am the person whose name appears on the vote-by-mail ballot envelope. I understand that if I commit or attempt any fraud in connection with voting, or if I aid or abet fraud or attempt to aid or abet fraud in connection with voting, I may be convicted of a felony punishable by imprisonment for 16 months or two or three years. I understand that my failure to sign this statement means that my vote-by-mail ballot will be invalidated.
Voter's Signature
Address"

"UNSIGNED BALLOT STATEMENT
I,, am a registered voter of _____ County,

State of California. I declare under penalty of perjury that I requested and returned a vote-by-mail ballot and that I have not and will not vote more than one ballot in this election. I am a resident of the precinct in which I have voted, and I am the person whose name appears on the vote-by-mail ballot envelope. I understand that if I commit or attempt any fraud in connection with voting, or if I aid or abet fraud or attempt to aid or abet fraud in connection with voting, I may be convicted of a felony punishable by imprisonment for 16 months or two or three years. I understand that my failure to sign this statement means that my vote-by-mail ballot will be invalidated.
Voter's Signature
Address"

"READ THESE INSTRUCTIONS CAREFULLY BEFORE COMPLETING THE STATEMENT. FAILURE TO FOLLOW THESE INSTRUCTIONS MAY CAUSE YOUR BALLOT NOT TO COUNT.
1. In order to ensure that your vote-by-mail ballot will be counted, your statement should be completed and returned as soon as possible so that it can reach the elections official of the county in which your precinct is located no later than 5 p.m. on the eighth day after the election.
2. You must sign your name on the line above (Voter's Signature).
3. Place the statement into a mailing envelope addressed to your local elections official. Mail, deliver, or have delivered the completed statement to the elections official. Be sure there is sufficient postage if mailed and that the address of the elections official is correct.
4. If you do not wish to send the statement by mail or have it delivered, you may submit your completed statement by facsimile or email transmission to your local elections official or submit your completed statement to a polling place within the county or a ballot drop-off box before the close of the polls on election day."

13.4. Canvassing Provisional Ballots

13.4.1. Voting a Provisionally Cast Ballot

(a) At all elections, a voter claiming to be properly registered, but whose qualification or entitlement to vote cannot be immediately established upon examination of the roster for the precinct or upon examination of the records on file with the county elections official, shall be entitled to vote a provisional ballot as follows:

(1) An elections official shall advise the voter of the voter's right to cast a provisional ballot.

(2) The voter shall be provided a provisional ballot, written instructions regarding the process and procedures for casting the ballot, and a written affirmation regarding the voter's registration and eligibility to vote. The written instructions shall include the information set forth in subdivisions (c) and (d).

(3) The voter shall be required to execute, in the presence of an elections official, the written affirmation stating that the voter is eligible to vote and registered in the county where the voter desires to vote.

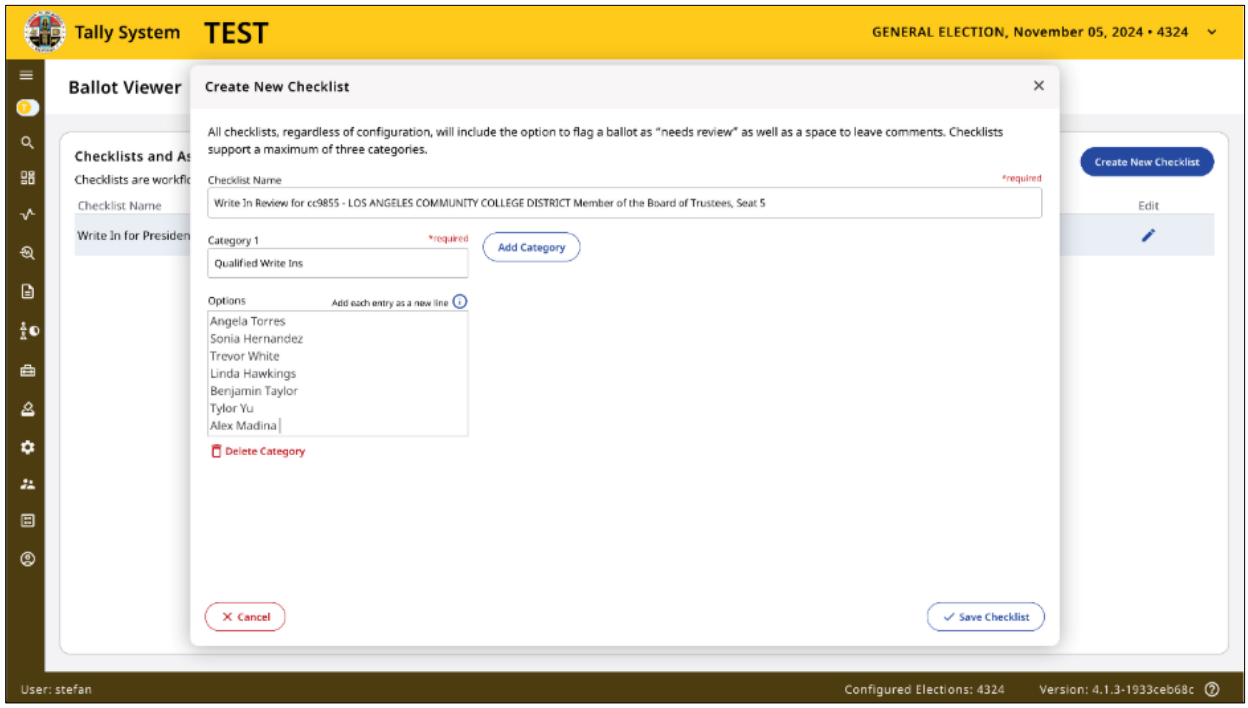
13.5. Canvassing Write-in Votes

13.5.1. Counting Write-In Votes

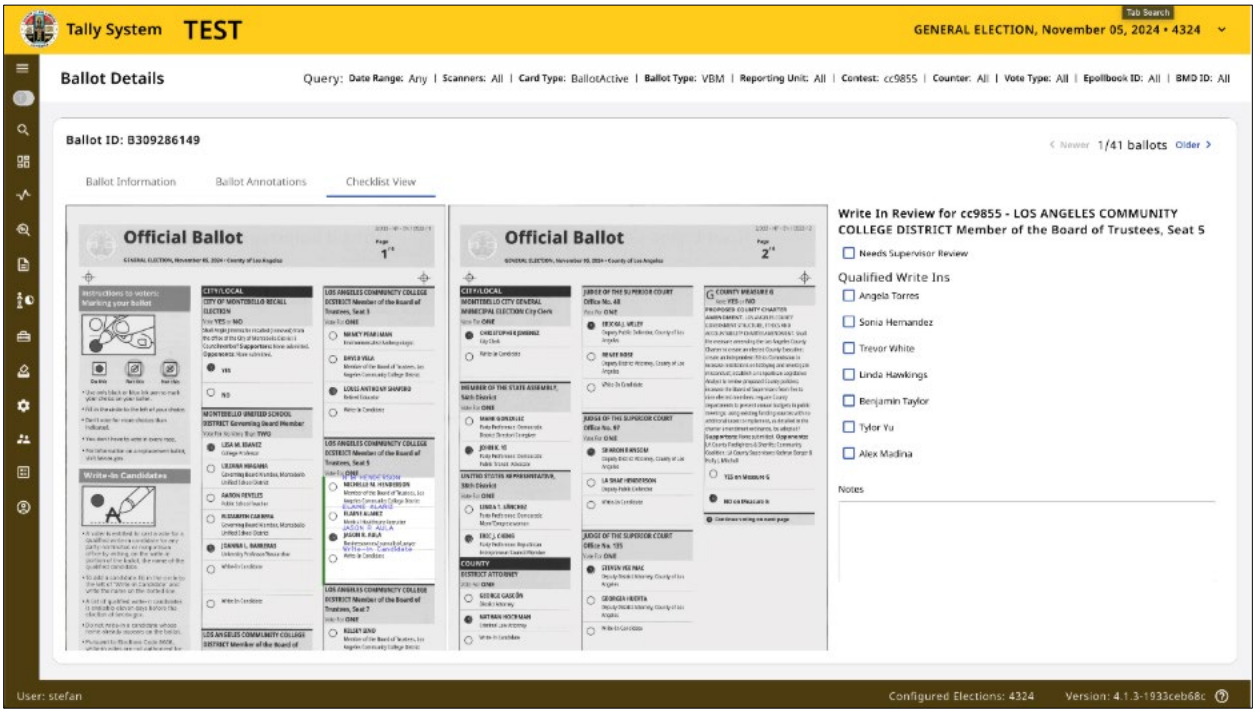
Any name written upon a ballot for a qualified write-in candidate, including a reasonable facsimile of the spelling of a name, shall be counted for the office, if it is written in the blank space provided does not exceed the vote for rule.

Ballot Viewer provides a way to view ballots that have been processed by Tally. Along with the ballot image, it also displays metadata extracted from the ballots by Tally. This functionality makes it possible to review write-in entries by contest.

Within the Ballot Viewer module, select the contests you want to review for write-ins and create a new checklist. Name your checklist, and under Category 1 select "Qualified Write-Ins." Under Options, add the qualified write-in candidates. This will make the qualified candidates selectable in the Ballot Viewer. When finished, click "Save Checklist.



In Ballot Viewer, select the name of the checklist. A list of ballots will appear, each linked to its corresponding ballot image. Select the ballot you want to view, and it will display with the contest for review highlighted by a green bar. Choose the qualified candidate, or select Older to move to the next ballot. Your selections will be saved automatically when you proceed to the next ballot.



13.6. Manual Tally Procedures

13.6.1. Manual Tally Using a Voting System

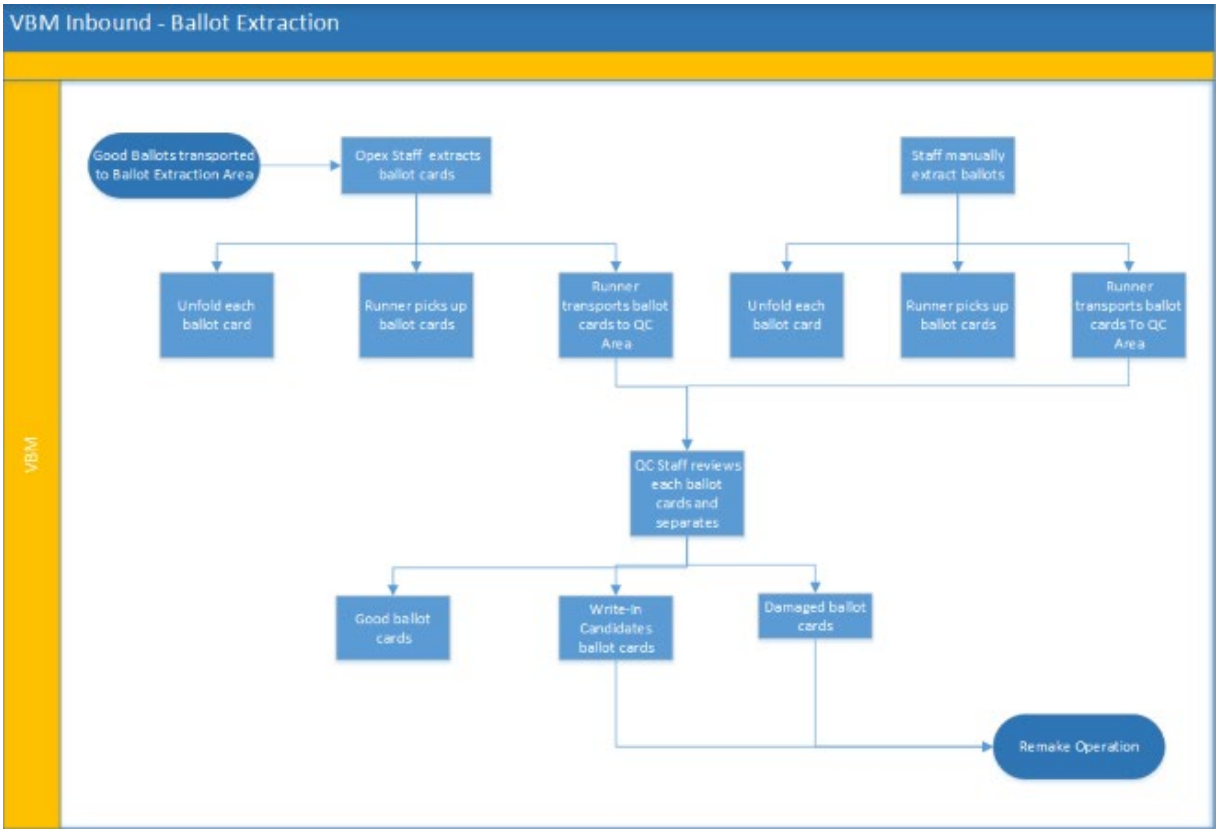
During the official canvass of an election, the elections official must conduct a public manual tally of ballots to verify the accuracy of the voting system. This may be done by randomly selecting batches or boxes representing 1% of the ballots cast for a manual count, with additional contests included as needed. The manual hand count is then compared to the Tally system results on a batch- or box-level basis in order to identify and report any discrepancies. The random selection process must occur at the start of the canvass, using methods approved by the Secretary of State, and the tally must be publicly noticed at least five days in advance. The results, including any discrepancies and how they were resolved, must be documented in the certified canvass, which serves as the governing record in the event of conflicts.

Box Tabulation is a function in Tally that is accessed through the tabulation menu. Once a box is selected, its number can be entered into the Box Number field, and a report is generated showing that box's results.

If a box that does not exist is entered, an error message notifies the user that the box does not exist for the election.

Figure: *Error message for box that does not exist*

13.7. Ballot Adjunction



The Tally System Recognizer determines if a vote mark is selected or not. The Recognizer uses vote mark detectors to find all vote positions defined by the Tally Layout Definition File (TLDF) for the ballot style of each card. When calculating whether a vote mark should be considered as selected or not, the recognizer assesses a variety of metrics including, but not limited to:

- If the vote circle could be found
- The computed skew of the vote circle relative to the expected position
- The number of dark pixels inside and outside the vote circle

- The darkness of those pixels

These factors are combined and weighed independently to validate that the vote position was confidently found and whether it should be counted as a vote. If the Recognizer is uncertain about the quality of the scan or the system's ability to accurately interpret the scan, it will outstack the card for human review. In cases where voter intent does not match how the ballot was marked, Tally's ballot adjudication tool can be used to make corrections if needed.

Digital Adjudication in Tally allows administrators and adjudication users to review and revise ballot selections for one contest at a time within the Ballot Viewer. Admins first define the contest to be adjudicated, then associate one or more searches that identify the ballots requiring review. Once a search is linked to a contest adjudication, users can begin reviewing ballots, with the system tracking whether each has been reviewed, flagged for supervisor review, or commented on. If ballot selections are updated, the system records the username and date of the most recent change.

For Digital Adjudication users to begin reviewing ballots with the selected contest, admins must associate one or more searches with the contest adjudication.

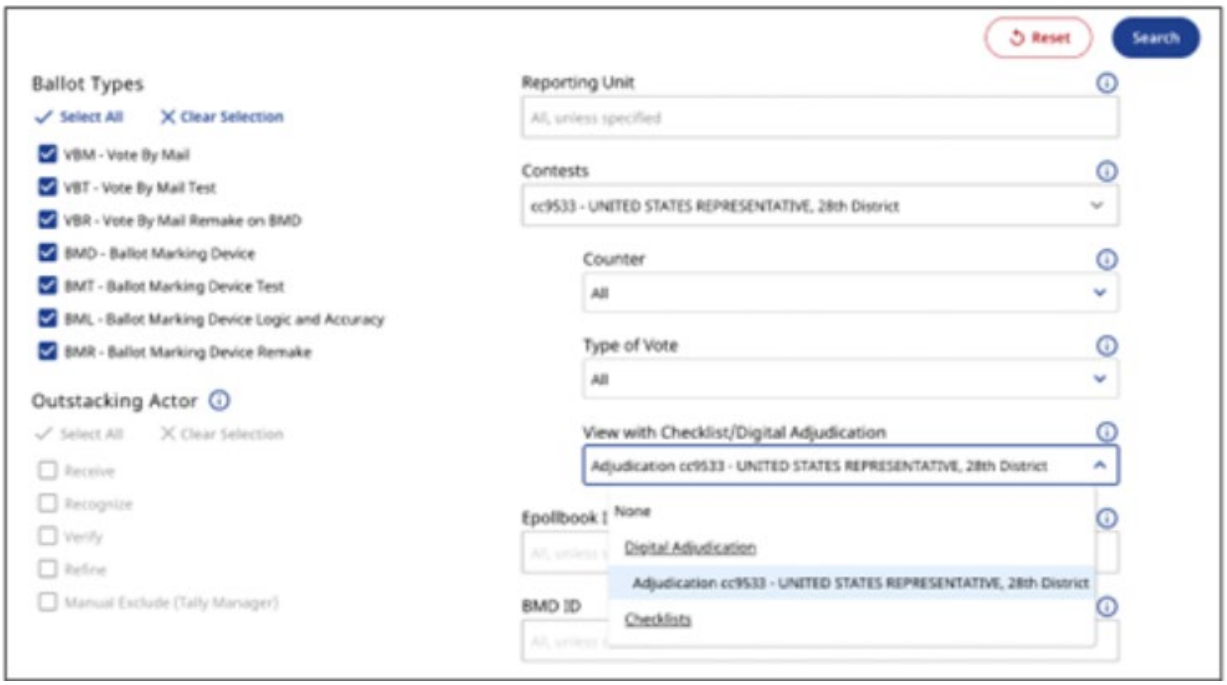


Figure: *Selecting to view selected search parameters with a Contest Adjudication (the first step to associating a search, and in part cards, to a Contest Adjudication)*

Saving the search to the contest adjudication: The search results will open in a new tab and display as usual with the header of the page saying "Viewing with Adjudication: [Contest Name]" and a button that will save the search to said contest adjudication. If the search parameters and results are as expected, clicking the **Save search to current adjudication** button will associate the search to the selected contest adjudication. This screen provides admins with a chance to confirm the search parameters and results before committing the search to the Contest Adjudication.

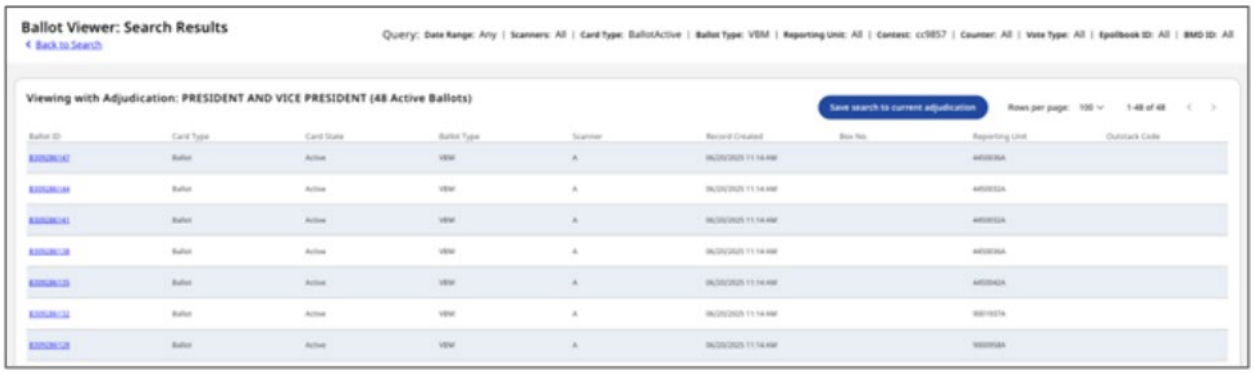


Figure: *Reviewing search results before saving search to current Contest Adjudication*

Once a search is successfully saved/associated with a Contest Adjudication, additional columns will be added to the results table:

- Reviewed: Can be either checked or empty. A check icon means that the ballot has been reviewed by a user in the context of this Contest Adjudication. If the column is empty this means the ballot has not yet been reviewed in the context of this Contest Adjudication.
- Needs Supervisor Review: Can either have a flag icon or empty. A flag icon means that the ballot has been reviewed and that a user flagged the ballot to be reviewed by a supervisor.
- Has Comment(s): Can be either a comment icon or empty. A comment icon means that a previous reviewer left a comment on that ballot.
- CVR Updated: This column will include the username and date if the ballot selections were updated as a result of this Contest Adjudication. If a ballot encounters multiple changes to the selections, the username and date displayed will be that of the most recent CVR update.

13.8. Adjudicating a Ballot

After at least one search has been associated with the Contest Adjudication, Admin or Digital Adjudication users can begin adjudicating those ballots associated with the Contest Adjudication via the search. Navigate to the Digital Adjudication tab on the Ballot Viewer page and click the “open modal” icon in the Saved Searches column for the desired Contest Adjudication. This will open a modal with all searches associated with the clicked Contest Adjudication. In addition to the search parameters of the associated search, the table presented will also provide helpful information regarding the progress of work across each of the associated searches. This includes the number of cards in the search, the number of cards that have been reviewed, the number of cards that require supervisor review, and the number of cards adjudicated (selections updated).

Figure: *Reviewing searches associated with a Contest Adjudication prior to adjudicating ballots*

To the right of the ballot image, users are presented with a number of tools to perform their adjudication:

- Needs Supervisor Review Checkbox: Users can check this box to notify an Admin that this ballot requires additional review by a supervisor.
- Max selections allowed: Informs the user what the max vote-for rule was for the contest being reviewed.
- Adjudicating Full Face Ballots: The vote for rule will not prevent the reviewer from making more selections than the contest allows. Reviewers can adjudicate selections to exactly match voter intent, including overvoting.
- Adjudicating Selections Only Ballots: Tally will prevent reviewers from adjudicating to more than the vote for rule. By definition, ballots from a Ballot Marking Device cannot be overvoted.
- Selection Table: Provides users with information regarding the selection that Tally detected, the most recent adjudicated selection (if any), and checkboxes for the user to perform their own adjudication.
- Notes section: An optional text box for users to leave comments for other reviewers.
- Reset button: Reverts the adjudication form to the same state it was when the page was loaded.
- Save and Next button: Save any selections or notes made in the adjudication form, makes a record that the ballot was reviewed, and takes the user to the next ballot in the search results list. Save and Next should be clicked even if no adjustments were made as a confirmation, by the reviewer, that the current selections are correct.
- Adjudication History: List of every review record associated with the ballot including information about the reviewing user and any adjustments made.

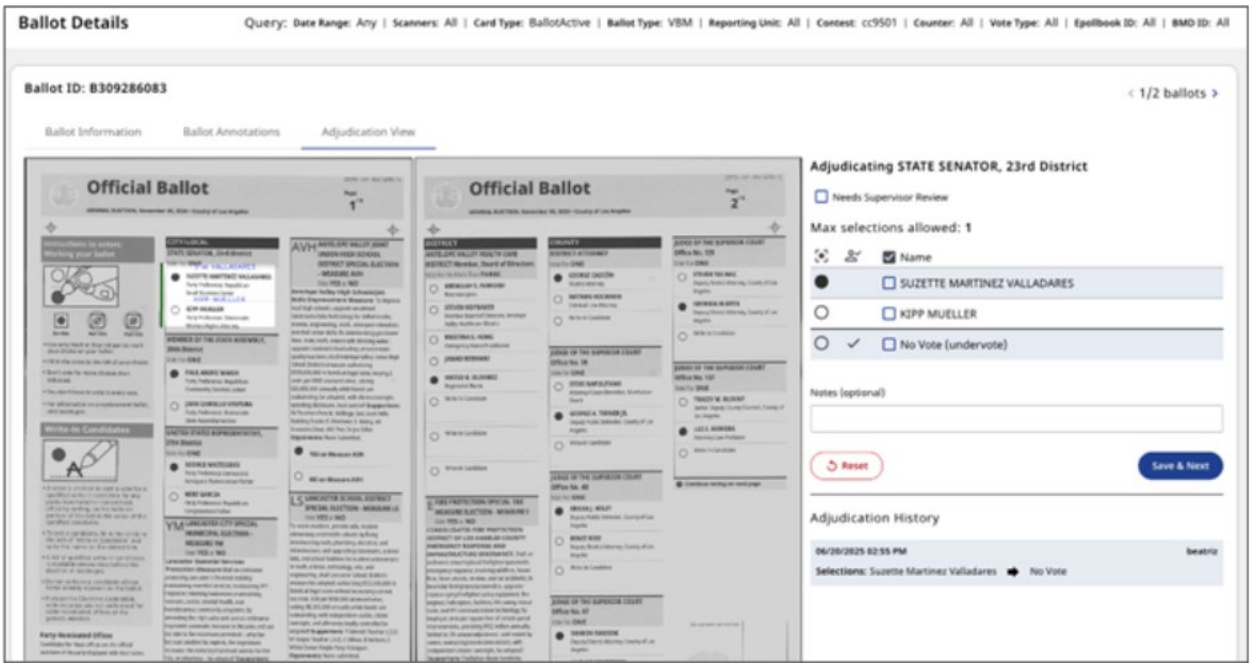


Figure: *Adjudication View for VBM ballot with one adjudication record updating the CVR to a no-vote*

13.9. Post-Election Logic and Accuracy Testing

After an election, Logic and Accuracy testing must be conducted to ensure the ballot layouts are correct and scanning equipment is accurate.

13.10. Final Reporting of Official Canvass

13.10.1. Sealing of Ballots

After ballots are counted and sealed, the elections official may not open any ballots nor permit any ballots to be opened except as permitted by law or in the event of a recount.

13.10.2. Results

(a) The elections official shall prepare a certified statement of the results of the election and submit it to the governing body within 30 days of the election or, in the case of school district, community college district, county board of education, or special district elections conducted on the first Tuesday after the first Monday in November of odd-numbered years, no later than the last Monday before the last Friday of that month.

(b) The elections official shall post the certified statement of the results of the election on his or her Internet Web site in a downloadable spreadsheet format that may include, but is not limited to, a comma-separated values file or a tab-separated values file and that is compatible with a spreadsheet software application that is widely used at the time of the posting. The certified statement of the election results shall be posted and maintained on the elections official's Internet Web site for a period of at least 10 years following the election. This subdivision shall apply only to an elections official who uses a computer system that has the capability of producing the election results in a downloadable spreadsheet format without requiring modification of the computer system.

When ballots are counted, the result of the vote shall be shown by precinct.

(a) The statement of the result shall show all of the following:

(1) The total number of ballots cast.

(2) The number of votes cast at each precinct for each candidate and for and against each measure.

(3) The total number of votes cast for each candidate and for and against each measure.

(b) The statement of the result shall also show the number of votes cast in each city, Assembly district, congressional district, senatorial district, State Board of Equalization district, and supervisorial district located in whole or in part in the county, for each candidate for the offices of presidential elector and all statewide offices, depending on the offices to be filled, and on each statewide ballot proposition.

13.10.3. Transmission to Secretary of State

The elections official shall send to the Secretary of State within 31 days of the election in an electronic format in the manner requested one complete copy of all results as to all of the following:

(a) All candidates voted for statewide office.

(b) All candidates voted for the following offices:

(1) Member of the Assembly.

(2) Member of the Senate.

(3) Member of the United States House of Representatives.

(4) Member of the State Board of Equalization.

(5) Justice of the Court of Appeal.

(6) Judge of the Superior Court.

(c) All persons voted for at the presidential primary. The results for all persons voted for at the presidential primary for delegates to national conventions shall be canvassed and shall be sent within 28 days after the election.

(d) The vote given for persons for electors of President and Vice President of the United States. The results for presidential electors shall be endorsed "Presidential Election Returns" and shall be canvassed and sent within 28 days after the election.

(e) All statewide measures.

(f) The total number of ballots cast.

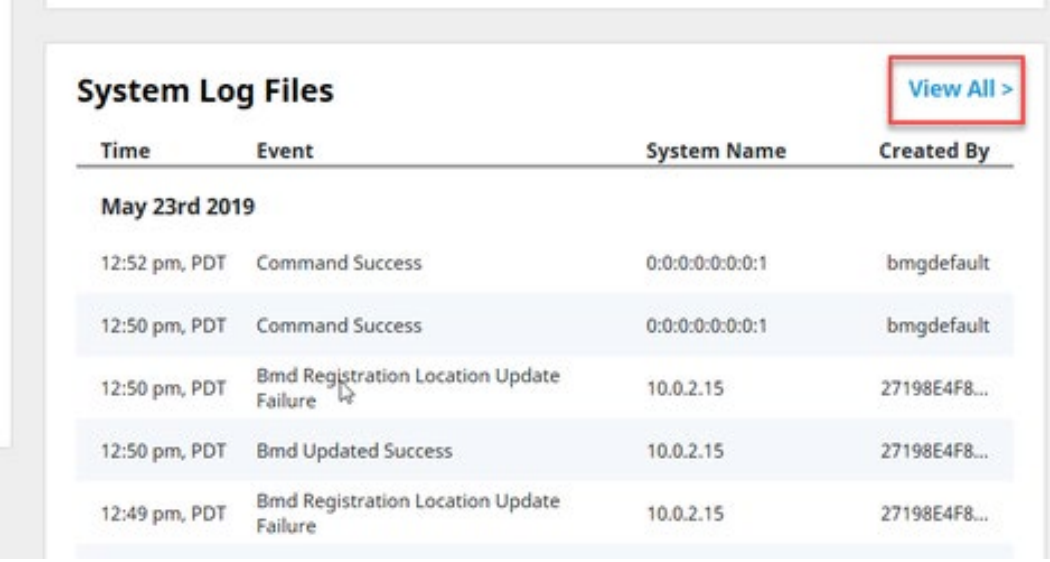
The elections official shall deliver a duplicate of the certified statement of the result of votes cast to the chairperson of the county central committee of each party.

13.11. Backup and Retention of Election Material

After an election, various logs and files must be downloaded and saved; see sections below to learn how.

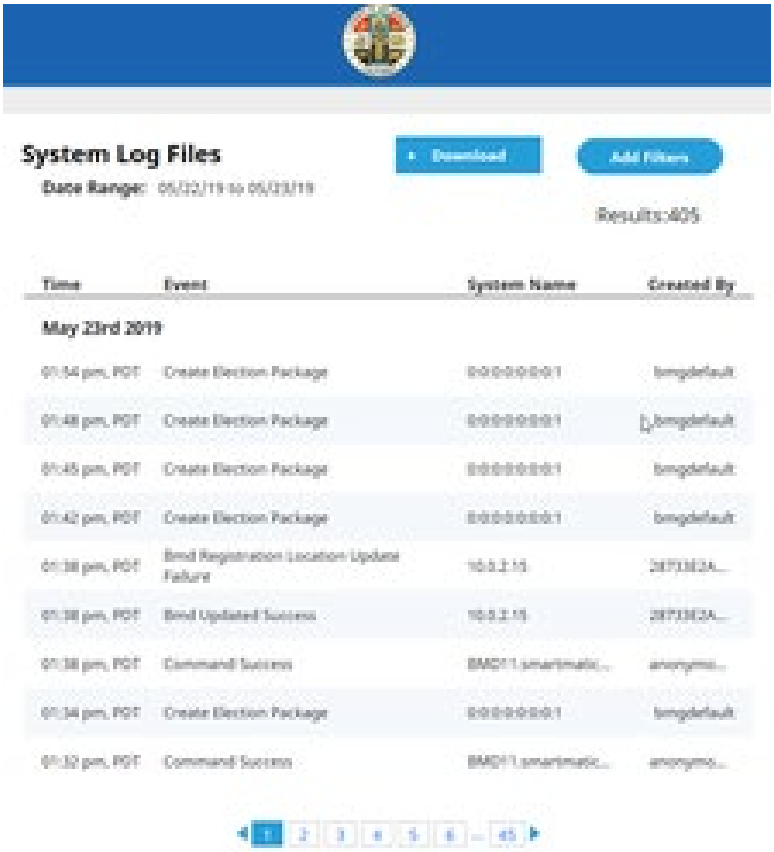
13.11.1. BMG

You can download a system log of events that took place in BMG. An Event is defined as any sort of system action that occurred on BMG. This includes any and all actions that were run on BMG, from user log-ins, diagnostic checks, BMD uploads and downloads, or any other actions taken on the BMG system. You can view and download these logs, filtered by certain criteria, by following the instructions below.



A list of all system events appears with a description of the event, the time it occurred, and who performed the event

1. From the BMG home page, in the System Log Files section, click View All



2. Click Download and choose a log file format, or click Add Filters. If no filter specification is selected, the system downloads a log of every single action by default

3. Click the dropdown button below to learn more about the different filters you can use

13.11.1.1. Filter Types

Filter by Date

Users can specify a specific date range for the logs you'd like to see.

Filter By Created By

Users can see a log of actions performed by specific users.

Filter By System Name

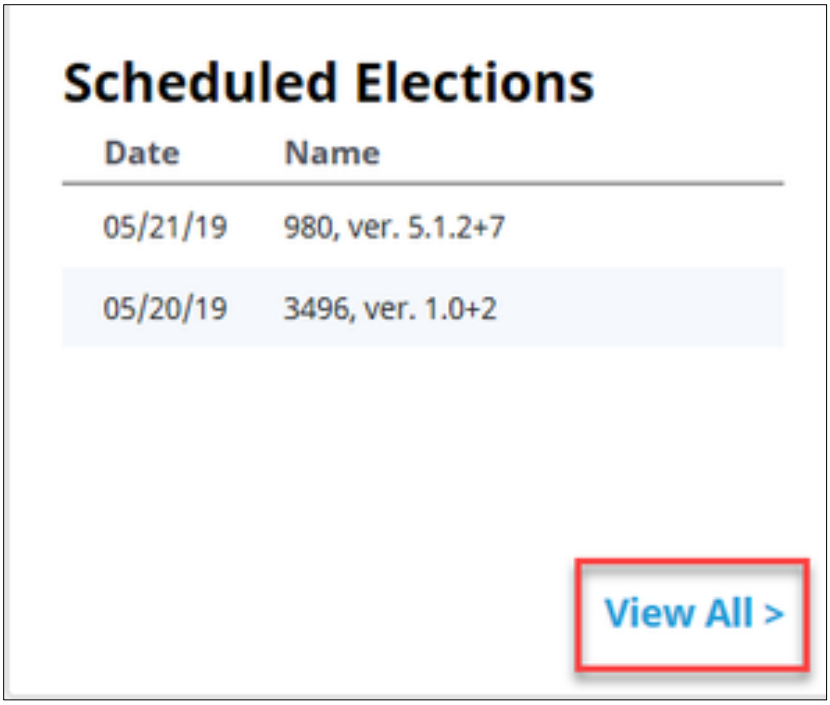
Each type of action is given a specific system name by the BMG system. If you know the system name for the type of action you're looking for, you can enter it here.

Filter By Events

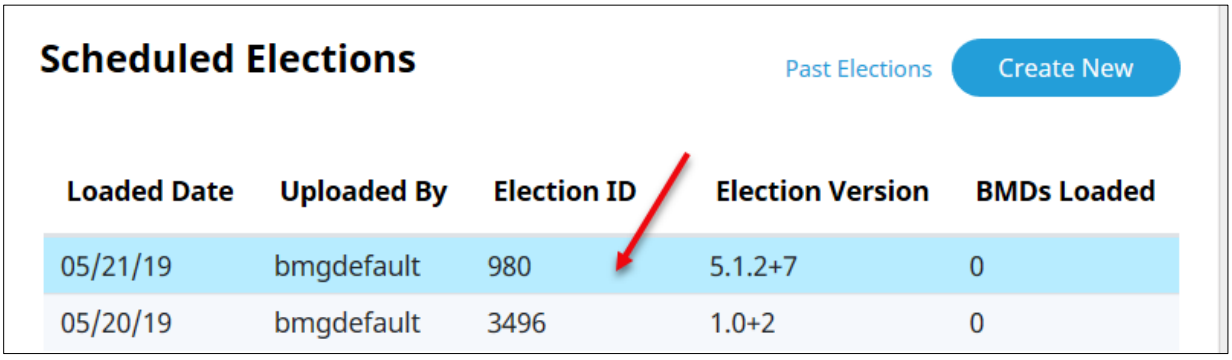
There is a filter by the type of action taken.

13.11.2. BMD Logs

After an election is over and the BMD devices have returned, it's time to download the election logs and keys from the devices. The election logs don't record any personal voter data, or any of their ballot selections during the voting process. The logs are simply a collection of the different BMD settings that were made by users, such as volume level, screen brightness, language settings, etc. Reviewing these logs allows developers to enhance the voting experience during the next election by gaining a sense for which BMD functionality settings might need to be updated to be more in line with the settings selections of the average user. The following steps describe how to collect logs using the BMG.



1. From the BMG main page, in the "Scheduled Elections" section, click View All



A page opens with a list of all upcoming elections that have already been scheduled

2. Click on the election ID and version whose logs or keys you'd like to download

3. Click Show Previous to view a list of elections that have already passed
4. Click either Aggregate Keys, or Aggregate Logs

If logs or keys are available for download, a new page opens with the option to download the files

5. Click Download
6. Depending on your computer settings, you will be asked to either download the file, or open it without downloading it
7. Transfer the files to a USB and give it to a Tally representative for processing

14. Manual Recount

Manual Recount Requests should be made in accordance with the California Elections Code and California Code of Regulations Chapter 8.1, including the jurisdictions Recount Procedures that are on file with the Secretary of State.

15. Security

15.1. Physical Security of System and Components

The System Security describes the voting system security. The system features access control mechanisms, equipment and data security, software installation and security policies, air gap policies, event logging details, physical security structures, specifications, standards, and regulations designed to protect the voting process from malicious attacks, data breaches, and accidental security incidents.

Network - The network domain that hosts election definition and ballot layout functions is physically separate from system and does not have inter-connectivity of traffic between domains. Data is transferred through a manual process under human control. The system is hosted on a separate network domain that is not physically connected to any other County LAN and no physical interconnections exist between the system and any other network or end-point device that connects to the Internet.

Protective Barrier - The placement and design of the room where the system and components are housed must allow for a secure environment that aims to deter or delay any attempt to disrupt operations while providing a means for interested parties to observe.

Rack-mounted Equipment - Hardware components such as scanners, servers and network devices must be housed in locked enclosures that contain racks for servers, network switches, power distribution units, and other components or peripherals. Serialized tamper-evident seals are used on removable panels. Removal and replacement of seals must be witnessed by at least two election staff members and documented using a log with signatures by both parties.

Access Control - Entry and Exit doors are restricted. A security guard should ensure that only employees with badges or escorted visitors are allowed to enter the facility. Policies and procedures for access control to the tabulation room must be defined and implemented.

System	Method	Description	Specifications
BMD	Trusted Platform Module (TPM)	The trusted platform module prevents unsigned software from signing onto the system	The TPM, a secure crypto-processor, integrates cryptographic keys into the BMD
BMG	Network Access Control	HP Aruba ClearPass: MAC address control, prevents non-authorized computers from accessing network	Tracks the machine MAC addresses of all computer network cards present on the network and removes any unauthorized network card MAC address from a network
ESA	Two-factor authentication with smart card	Radio Frequency Identification (RFID) limits access to the HSM	The smart card RFID is issued to an authorized individual, which serves as a part of two-factor authentication.
ISB	Network Access Control	HP Aruba ClearPass: MAC address control, prevents	Tracks the machine MAC addresses of all computer network cards present on the network and removes any

System	Method	Description	Specifications
		non-authorized computers from accessing network	unauthorized network card MAC address from a network
Tally	SSH Key Authentication	Cryptographic key pairs to establish identity and authorize access	Industry standard algorithms with all communications encrypted via SSH protocol
VBL	SSH Key Authentication	Cryptographic key pairs to establish identity and authorize access	Industry standard algorithms with all communications encrypted via SSH protocol

15.2. Logical Security of System and Components

15.2.1. Essential and Non-Essential Services and Ports

Unused USB data ports are covered with serialized tamper evident seals on the VSAP servers and related components. USB port locks are physical blockers designed to safeguard servers and desktops from the connection of unknown devices. They offer additional security and access is monitored by the county security team.

Component	Ports and Access Points
BMD	USB port, Ethernet port, 3 x 3.5 mm ports
BMG	USB port, Ethernet port, 3.5 mm audio, HDMI, SD card reader, and VGA HPE ProLiant DL830 Gen10: Display Port 1, 8 LFF chassis standard Flexible LOM Network Ports, 4 x 1 Gb ports, HPE iLO Remote Management Network Port, 1 Gb Dedicated Front iLO Service Port, Micro SD Slot 1 Micro SD, USB 3.0: 1 front, 2 rear, 2 internal (secure) HP 8320 JL479A: 48p 10G SFP/SFP+ and 6p 40G QSFP+ Switch HP8320 JL579A: 32p 40G QSFP+ HP3810M JL075A: 16 SFP+ fixed 1000/10000 SFP+ ports; Duplex: 100BASE-TX: half or full; 1000BASE-T: full only; Ports 1 – 16 support MACSec HP2930F JL253A: 24 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/ 100BASE-TX: half or full; 1000BASE-T: full only; 4 SFP+ 1/10GbE ports; PHY-less HP2530-8G JL9777A: 8 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Media Type: Auto-MDIX; Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only; 2 dual-personality ports; each port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-Tx; IEEE 802.3ab 1000Base-T Gigabit Ethernet) or as a SFP slot (for use with SFP transceivers) ports
ESA	Intel NUC7i7DNHE: USB, SATA, Ethernet nShield Edge F2 HSM: SD card reader and USB

Component	Ports and Access Points
ISB	USB port, Ethernet port, 3.5 mm audio, HDMI, SD card reader, and VGA
Tally	Compute servers: USB, Ethernet, Video/display, PS2, Audio Scanner machines and scanner support machines: Ethernet, Video/display, PS2, Audio, Imprint Storage Appliance: Ethernet, Audio Workstations: USB, Ethernet, Video/display, PS2, Audio Switches: Various network
VBL	Compute server: USB, Ethernet, Video/display, PS2, Audio Workstations: USB, Ethernet, Video/display, PS2, Audio Switches: Various network

15.2.2. User-Level Security

The system has numerous access controls to deter unauthorized users from accessing the system. There are three role types in the system. The first role is the Linux administrator. The Linux administrator can configure the system, setup new users, set up configuration files, configure the system, and view logs. Second is the application admin. The application administrator can manage running services in the system, tabulate elections, view errors, and conduct all necessary election night operations. Finally, is the view-only user who can look at the Manager interface, but cannot physically affect the system.

The system is only accessible to individuals who have a username and password. Usernames and passwords are managed via process by the system administrator. User passwords are never stored in clear text or reversible formats in unencrypted storages. There is a system tool for generating password entries. All user passwords are stored with password encoder software. These files are protected via file permissions.

15.2.3. Anti-Virus Protection

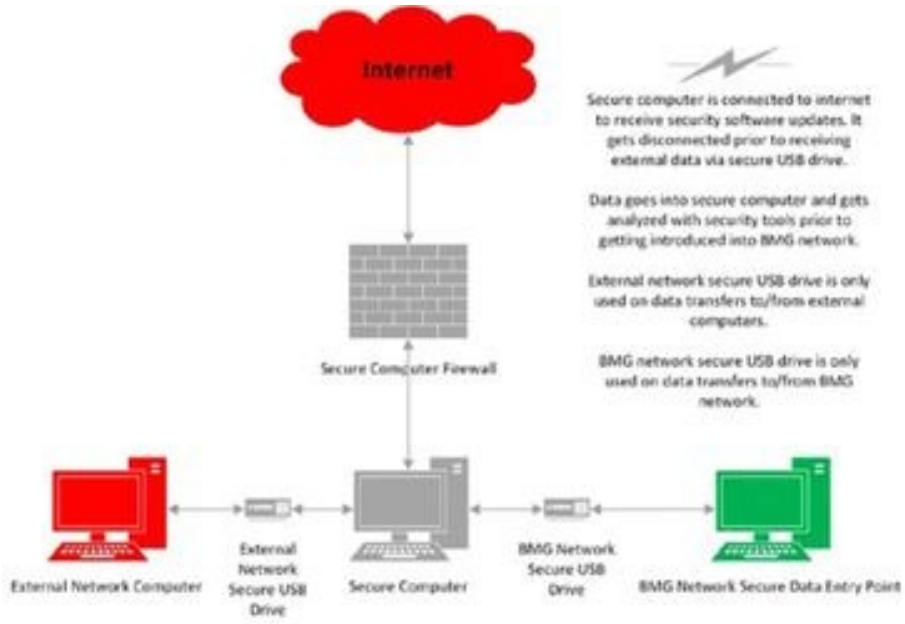
System security in an air-gapped environment:

- Carbon Black Protect Software (CB Protect): This software once installed, takes away elevated privileges on any operating system. All software on a computer system with CB Protect installed is subject to permission from it to execute. This software functionality reduces the chances of malicious software to run on a computer. However, it is strongly advised to have Smartmatic assist in the install of this product in the air-gap environments and for CVSS testing. Any mis-configuration can interfere with the proper operation of software on a computer system.
- HP Aruba ClearPass: Tracks the machine (MAC) addresses of all computer network cards present on a computer network. The software, in addition to monitoring MAC addresses, can remove any network card MAC address from a network that is not authorized to be on that network. This software function disrupts any attacker from placing implants or connecting workstations to any air-gap network without authorization.

It is recommended that application validations, such as functionality and performance testing, be carried out by BMG application specialists and BMG technical teams after software is installed on any air-

gapped network. If software is improperly configured (CB Protect for instance), it can disrupt proper operation of the computer network.

- Graylog SIEM collects and analyzes computer system and network activity by aggregating logs from various devices, systems, and applications across the environment. These records can be retained for several years, depending on the available storage capacity and configured data retention policies. Graylog serves as a centralized method for monitoring, auditing, and reviewing network activity, particularly in the event of a security incident or operational issue. Graylog does not alter or tamper with log data during collection or storage. Logs are ingested and stored in their original form, ensuring that the integrity of the data remains intact by default. However, maintaining this integrity depends on implementing proper security measures such as access controls and secure storage configurations. It is recommended that Graylog and/or experienced security professionals oversee the installation and configuration of the system, especially in air-gapped or sensitive environments.



15.2.4. Verifying, Checking, and Installing Essential Updates and Changes

Changes are primarily for installing critical updates to the operating system, anti-virus protection, or other third-party elements related to security and error correction.

15.3. Event Logging Capabilities

15.3.1. BMD

A usage data collection log file records executed events on the device; audit logs will record every event triggered in the BMD as one of the following types: info, error, warn, fatal, and debug. Logging is performed in the voting app. The BMD Interaction Data (BID) is a fixed-sized usage log that counts ballots cast. The BMD Election Log (BEL) is an audit log that creates separate records for each user interaction.

The BMD allows multiple BELs for multiple elections. All logs are written to the data partition.

15.3.2. BMG

The BMG contains a file-based audit logging system. Timestamps will be generated in the format ISO8601 including time zone (e.g. 2017-09-26T01:57:58+00:00). Event logs are stored and reported through Graylog.

15.3.3. ESA

The ESA uses a file-based logging system. The ESA program and scripts write system logs to a text file located on a central Unix directory. Log files can be read using standard Unix text processing commands such as less and cat. Since the ESA is intended to be used only occasionally and for limited numbers of tasks, log files are not expected to grow significantly, eliminating any need for rotating files.

15.3.4. ISB

The ISB logs specific events to a log file, including:

- System ID
- Unique event ID and/or type
- Timestamp
- Success or failure of event, if applicable
- User ID triggers the event, if applicable
- Resources requested, if applicable

The ISB will use AWS S3 for storage of the statically hosted log files. It will employ encryption and will have AWS CloudTrail logs enabled.

15.3.5. Tally

Tally uses Graylog to log and monitor system events.

15.3.6. VBL

VBL uses Graylog to log and monitor system events.

15.4. Event Logging Design and Implementation

15.4.1. BMD

To facilitate security and traceability of the BMD, logging capabilities are designed to capture information about each unique event, including: sequence number, unique event ID, transaction results, user and event types, average voting session time, and event occurrences.

SSD has four data usable partitions, one of which stores logs (Data partition). Diagnostic (pre-setup) has logs, then logs are captured while users are voting; then they’re unpacked or read back at the warehouse when connected to BMG.

15.4.2. BMG

For daily logs are aggregated into CSV files for exported for any period. Additional integration such as Graylog and Elasticsearch is also possible.

The system information and event management (SIEM) software provides an audit trail through continuous logging of network activity. The system uses Graylog as its SIEM, providing detailed log data for the network. This data is suitable to provide actionable intelligence and critical insight both for security monitoring and incident response forensics. These products are also capable of reporting a summary overview.

15.4.3. ESA

Testing output, event logs, and error logs are all stored in a local log file.

15.4.4. ISB

AWS access logs stored in the S3 bucket.

15.4.5. Tally

Each Tally service logs events to the file system and makes them available through the SIEM along with log files generated on the file system of the servers The logs are preserved for auditing and are included backups taken of the environment. Backups include all election specific logs and general logs that have been generated at the moment the archive is requested. Rotation of logs is set for each service and is used to preserve disk space as logs grow over time. The system will never remove old logs automatically, this operation must be done by an approved operator to ensure proper data retention.

15.4.6. VBL

Each VBL service instance logs events to logs on the file system. The logs will be preserved for auditing. The system will never remove old logs automatically, this operation must be done by an approved operator to ensure proper data retention.

15.5. Installation Procedures

The system is hosted on a separate network domain that is not physically connected to any other County LAN and has no physical interconnections existing between the system and any other network or end-point device that connects to the Internet. The application runs on a standalone COTS PC and is physically separated from the system. Data between the two systems is transferred through a manual process under human control and performed by trusted staff. Installation of updates is performed through a set of manual procedures overseen by trusted election managers. Installation activities are documented with at least two staff members performing updates. Documentation includes date-time of update, person who performed activity, person who witnessed the activity, and certification that update installed was previously approved.

15.6. Security Procedures for the BMD Warehouse

Physical security standards for all persons working or entering the BMD Warehouse. These policies comply with NIST 800-171 Physical Protection, Media, and Personal Security Policies.

Authorization is required to enter the BMD Warehouse. The following are the only authorized personnel:

- Select, jurisdictionally appropriate, personnel
- Approved contractors
- Building maintenance personnel

The following personnel are authorized, but may be subject to the jurisdiction's escort and monitor policy:

- Vendors (including delivery personnel)
- Visitors

Valid ID badges are required to enter the BMD warehouse and must be worn and visible when one is inside the building. Visitors will be expected to have temporary badges distributed from the visitor management system. Any person without a badge showing authorization is considered an adversary and will be escorted to the security desk immediately.

Employees will report a badge that's been lost, stolen, or compromised in any way, to the security office. Visitors must engage an employee related to the visitor management system upon final exit of the building, as temporary badges will be collected at the end of each visit.

Refer to jurisdictional procedure guides for further information on existing guidelines governing identification of personnel entering Information Technology areas.

Cameras will monitor all areas of security concern:

- Truck and delivery yard
- Employee parking
- Visitor center entrances
- Employee entrances
- Warehouse for BMDs
- BMD repair facility
- Kitting area

The facility will create protected yards for employee parking, and facilities for trucks and large equipment.

- Gates and fences will protect the warehouse loading bays from being penetrated by unauthorized persons
- Gates will be monitored by site security personnel

Employee physical access will account for tailgating, which is when an unauthorized person gains access by trailing behind authorized personnel.

- The employee entrance area will also be monitored by cameras. In addition to monitoring, these cameras will remind employees to be vigilant regarding security while inside the facility

Video will be accessible from inside the facility. Proper authentication will allow for secure access by jurisdictionally appropriate security personnel and the local sheriff's office, as well as from inside the facility.

A burglar alarm will be configured to detect any unauthorized entrance to the facility. The final design of the security system will be determined based on the characteristics of the facility selected for the BMD warehouse.

All USB media are to be serialized and tracked to individual users via a checkout sheet maintained by the IT Security Staff.

The server\switching rooms shall have restrictions on phones and employee-owned personal electronics inside those areas. The individual devices restriction policy shall be enforced by BMD warehouse staff via written policy. No employee-owned smartphone or personal electronic device will be allowed inside critical air-gapped server rooms or server areas connected to the electronic poll books. All employee-owned electronic devices shall be kept in lockers placed outside of the server rooms. Failure to follow the policy should result in disciplinary action from the BMD warehouse management staff.

- Employee-owned electronic devices can be compromised by improper security, or by the term of service agreements for applications on the phone.
- Terms of service or improper activity may cause cameras, microphones, and the GPS data in the device to be turned on and used for surveillance of restricted sites, without the knowledge or permission of the owner.

Adherence to the following procedures is required:

- All BMD Warehouse employees are expected to keep a clean workstation area
- Any documents related to the voting operations will be in a locked drawer or other secure areas when not in use
- Workstations screens are to be locked when employees are away from their computers by Windows group policy of no longer than five minutes
- Any removable storage devices must be locked in a protected area
- Any documents to be discarded must be shredded

Employees are not allowed to use personal devices to audio- or video-record any activity within the BMD Warehouse. Management must be notified to find a solution if an employee requires audio or video recordings. As stated earlier, it is possible via a term of service for photographs taken on a smartphone to be shared without the user's knowledge.

Only jurisdictionally appropriate or LA County approved computers are allowed to connect to the VSAP network facilities at any time.

All computers must be registered to the network access solution protecting the VSAP network. Any computer not known to the network access software will be restricted, and alerts will be sent to IT security staff immediately.

Personal storage and media devices are not allowed to be connected to computers. Security software will only allow connections by USB to devices designated by an appropriate local, state, or federal jurisdiction personnel. Restricted storage and media devices include:

- USB drives
- Flash drives
- Mobile phones
- Any other devices capable of recording

A vendor who brings these devices into the BMD warehouse must present them to IT security for malware scanning by the designated AI antivirus software. Any necessary or required data will be copied to a USB storage device issued by an appropriate local, state, or federal jurisdiction and provided to the vendor for the work required and returned at the completion of the work to the security desk. This provided storage device must be returned to IT security once the vendor has completed their task. The vendor then will retrieve their personal device. Any vendor who violates these rules will be subject to immediate removal from the BMD warehouse.

In some cases, IT security may authorize, issue, clear, and track media devices connected to BMD warehouse computers and servers. Any USB device or media shall be purchased by the appropriate local, state, or federal jurisdiction and security tested by IT security personnel prior to use in the network. Devices will then be assigned random serial numbers to verify they are safe to use.

Only serialized USB storage media managed and tracked by BMD warehouse security staff will be connected to VSAP equipment.

All computers not requiring a USB media connection, as determined by BMD warehouse security staff, will have their USB ports disabled by an endpoint security software or physically.

Any device used to connect to VSAP equipment without a serial number must be turned into IT security for examination.

Every quarter, the security staff will perform random tests to assess physical security and compliance with access procedures. It is strongly recommended that a "red team" of security evaluators test the facility after each election to determine security compliance.

15.7. Security Procedures for Vote Center

15.7.1. BMD Vote Center Storage and Security Seal

BMD devices will be delivered to the Vote Centers prior to Election Day. During transit, carts and storage containers are sealed with evidence tape and/or tamper evident seals. Access points to the BMD are outfitted with tamper evident seals with either or both tamper evident residue or visual appearance change to the seal itself to reveal modification or removal and to help prevent access or theft (see pictures below). The BMD ballot boxes are also outfitted with tamper evident zip-tie style seals utilizing signaling evident technology to reveal modification and/or removal. In addition, a tamper-evident seal is also placed over the seam at the top of the IBB (see picture below of tamper-evident seal). Removing, creasing, scratching of laminating the factory applied film exposes prominent "OPEN VOID" messages. Seals use Secure ID technology that has a distinctive metallic finish which serves as an anti-counterfeiting and authentication feature. In addition, BMDs will be kept in a secure location at each Vote Center. During overnight storage, BMDs should be stored in rooms that are sealed with evidence tape at access points and/or in rooms that can be locked with a key.

Integrated Ballot Box security seals

USB and Ethernet port security seal

All tamper evident seals are serialized and logged via established "chain-of-custody" procedures; this includes replacing and logging any need to break seal(s) for reason of entering a storage area, room, ballot box, or any other secured locale. An election inspector / overseer will verify that the correct seals are intact on the BMD containers, carts, and devices prior to set up, and use in the election.

15.7.2. Ballot QR Codes

The Ballot Page Metadata (BPM) QR code in the upper left-hand corner of the ballot contains information about current election status and indicates the ballot's originating BMD. BMDs assigned to the election pass their security keys to Tally; BMDs that are not officially part of the election will produce an error.

Additional security measures:

- An audit of each precinct's electronic tally of the number of votes cast will be conducted against the number of signatures in the precinct's ePollbook
- Vote center officials will be required to certify in writing that the proper locks and seals were found intact on the BMD devices, carts, and containers before the polls open. Exceptions and discrepancies will be reported to the Help Desk immediately upon discovery
- A physical inventory of all BMD devices will be conducted before and after each election to ensure custody of all devices is maintained and/or accounted for; there are functions within the BMG that can be used to aid in this inventory

16. Audit Trails

Election audit trails are vital to validating the accuracy of election results. All system components create an audit log anytime the system is accessed, or data is changed. Audit logs can be opened and printed to hard copy if needed.

16.1. BMD Log Files

The BMD logs significant system events during elections and anonymous usage data. This information is useful for auditing purposes and for ongoing user experience analysis. These logs are retrieved using the BMG.

Per federal law, County personnel must ensure retention for a 22-month minimum period of all election artifacts. This includes electronic records collected by the VSAP system such as: VBL, BMG, and Tally event logs and the aggregated BMD event logs.

Log File	Type	What it Tracks
BID - BMD Election Interaction Data	Audit	Information about the interactions between the voter and the system, such as: • Font size • Language • Voting system time • Only aggregate interaction data is recorded, not individual voter choices
BEL - BMD Election Logs	Usage	Each event triggered during the voting experience at the BMD, such as: • Shutdown • Empty ballot box • Cancel voting session

17. Biennial Hardware Certification and Notification

California Elections Code requires jurisdictions to inspect voting systems and certify their accuracy once every two years. All ballot marking devices, tabulators, scanners, elections management software, and supplementary equipment must be certified by California's Secretary of State prior to their use in any election taking place in California. In addition, all specialized tally equipment must be certified for use in elections by the Secretary of State prior to use in any election.

17.1. Notification of Software or Equipment

For every state election, the Election Official of the respective county is responsible for providing all the necessary files and documentation as defined by the California Election Code and certification use conditions. In the event of a change to the ballot tally program after certification, an amended certificate shall be submitted to the California Secretary of State no later than the day before the election. In the event any equipment is repaired, altered or replaced following the certification specified in this section, and prior to completion of the official canvass of the vote a list of changed equipment used must be submitted to the Secretary of State no later than official canvass submission.