

Statewide Voter Registration System Project

California Secretary of State

EMS Certification Plan

**Version 1.1**

March 2021

**REVISION SUMMARY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version #** | **Change Date** | **Author** | **Comment** |
| 0.1 | 4/17/2019 | Sean Malone | Initial Draft |
| 0.2 | 4/29/2019 | Sean Malone | Incorporated feedback from Sean Mooney regarding the Performance test plan and Code Deliverable |
| 0.3 | 5/21/2019 | Sean Malone | Incorporated feedback from Anna, Mike, and Harjit regarding section 3 |
| 0.4 | 6/29/2019 | Sean Malone | Added further description to the System test plan. Adjusted language for the Initial Software System Design Document. |
| 0.5 | 4/10/2020 | Sean Malone | Internal development and testing phase adjustments. |
| 1.0 | 3/10/2021 | Sean Malone | Various adjustments to staffing, system test and UAT phase updates. |
| 1.1 | 3/12/2021 | Sean Malone | Minor updates to startup materials provided |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**TABLE OF CONTENTS**

[1 Summary 1](#_Toc66445576)

[1.1 Scope 1](#_Toc66445577)

[2 Roles and Responsibilities 1](#_Toc66445578)

[2.1 Deliverable Review Responsibilities 4](#_Toc66445579)

[3 Certification Process 6](#_Toc66445580)

[3.1 Initiation 6](#_Toc66445581)

[3.1.1 Introduction 6](#_Toc66445582)

[3.1.2 Application to Initiate the Certification Process 8](#_Toc66445583)

[3.2 Planning 9](#_Toc66445584)

[3.2.1 Deliverable 1: Work Breakdown Structure 11](#_Toc66445585)

[3.2.2 Deliverable 2: Interim Software System Design Document 11](#_Toc66445586)

[3.2.3 Deliverable 3: System Architecture Document 11](#_Toc66445587)

[3.2.4 Deliverable 4: Performance Test Plan 12](#_Toc66445588)

[3.2.5 Deliverable 5: Security Test Plan 14](#_Toc66445589)

[3.2.6 Deliverable 6: System Test Plan 17](#_Toc66445590)

[3.2.7 Deliverable 7: Interim EMS Code Delivery Expectations 18](#_Toc66445591)

[3.3 Internal Development / Testing 19](#_Toc66445592)

[3.3.1 Deliverable 2: Software System Design Document 20](#_Toc66445593)

[3.3.2 Deliverable 3: System Architecture Document 21](#_Toc66445594)

[3.3.3 Deliverable 5: Security Test Plan 22](#_Toc66445595)

[3.3.4 Deliverable 6: System Test Plan 22](#_Toc66445596)

[3.3.5 Deliverable 7: Interim EMS Code delivery 23](#_Toc66445597)

[3.4 System Testing 23](#_Toc66445598)

[3.4.1 Execute System Testing 23](#_Toc66445599)

[3.4.2 Deliverable 2: Interim Software System Design Document 25](#_Toc66445600)

[3.4.3 Deliverable 8: System, Performance, and Security Testing Results 25](#_Toc66445601)

[3.4.4 Deliverable 7: Interim EMS Code delivery 26](#_Toc66445602)

[3.5 User Acceptance Testing 26](#_Toc66445603)

[3.5.1 Execute UAT 26](#_Toc66445604)

[3.5.2 Deliverable 2: Final Software System Design Document 28](#_Toc66445605)

[3.5.3 Deliverable 3: Final System Architecture Document 28](#_Toc66445606)

[3.5.4 Deliverable 4: Final Performance Test Plan 29](#_Toc66445607)

[3.5.5 Deliverable 7: Final EMS Code delivery 30](#_Toc66445608)

[3.5.1 Deliverable 9: User Acceptance Test Plan 30](#_Toc66445609)

[3.6 Final Certification 31](#_Toc66445610)

[3.6.1 Application for Initial Certification 31](#_Toc66445611)

[4 EMS Deliverable review process 33](#_Toc66445612)

[4.1 Definition of Deliverable Expectations: 33](#_Toc66445613)

[4.2 Pre-submission Review Activities 33](#_Toc66445614)

[4.3 Formal Deliverable Review 34](#_Toc66445615)

[4.3.1 Formal Deliverable Review assignment email template 36](#_Toc66445616)

[5 Ongoing Certification 37](#_Toc66445617)

[5.1 Re-Certification Process 37](#_Toc66445618)

[5.2 SOS Maintenance Contract agreement 38](#_Toc66445619)

[6 Appendix 39](#_Toc66445620)

[6.1 Acronyms 39](#_Toc66445621)

[6.2 EMS Certification Steps by Phase 40](#_Toc66445622)

**LIST OF TABLES**

[Table 1 – Deliverable Review Responsibilities 4](#_Toc66445567)

[Table 2 – Deliverable Review Roles 5](#_Toc66445568)

[Table 3 – Introduction Materials 6](#_Toc66445569)

[Table 4 – EMS Certification Materials 9](#_Toc66445570)

[Table 5 – Performance Requirements 13](#_Toc66445571)

[Table 6 – County Security Requirements 14](#_Toc66445572)

[Table 7 – Technical SOS-ITD connection requirements 19](#_Toc66445573)

[Table 8 – System Testing Defect Severity Definitions 24](#_Toc66445574)

[Table 9 – User Acceptance Testing Defect Severity Definitions 27](#_Toc66445575)

# Summary

Currently, there are two certified county Election Management Systems (EMS) in the state of California. California counties are dependent on these EMS to provide VoteCal the required updates to meet current Federal HAVA legislation and current California Elections regulations. Many counties using these EMSs have expressed the need for alternative options.

Since 2018, the SOS has been contacted by multiple new EMS vendors requesting to do business in the state of California. The EMS Certification Plan (ECP) outlines the steps and requirements for new EMS vendors to attain certification from the SOS for counties to use their EMS to integrate with VoteCal to meet HAVA regulations. The ECP also outlines the reoccurring certification requirements and process existing certified EMS vendors must follow to maintain their certification. Certification includes following the software development lifecycle to implement and verify new EMS’s that meet state requirements as well as a wide variety county requirements.

## Scope

This plan covers all steps and actions that are required for an EMS vendor to integrate their EMS with the VoteCal system and become certified to operate as an EMS representing counties in the state of California. The plan also outlines county responsibilities for the certification process. The intended audience for the ECP is the SOS VoteCal program team, new EMS vendors approved to begin the certification process, and counties working with EMS vendors.

# Roles and Responsibilities

Below you will find general responsibilities of EMS vendors, the SOS and Counties. In the remainder of the document you will find detailed responsibilities for all.

EMS new vendors:

EMS vendors attempting to get certified are responsible for implementing an EMS, or remediating an existing EMS, to integrate with the VoteCal application seamlessly and to meet county requirements and SOS VoteCal integration requirements, including state and federal regulations and legislative requirements. In-order to verify SOS VoteCal integration requirements have been met and that future investment of time and resources from the SOS is warranted, EMS vendors are responsible for submitting deliverables outlined in the remainder of this plan and SOS is responsible to review, provide feedback and/or approve each deliverable. EMS vendors are also responsible to provide representative counties with the deliverables, processes and/or mechanisms that will allow the county to verify that the EMS meets their county requirements.

EMS existing vendors:

Existing EMS vendors are responsible for meeting all ongoing certification requirements such as submission of updated code to escrow and yearly confirmation of VoteCal ongoing process participation and adherence to standards.

SOS Project Management Office:

The SOS Project Management office is responsible for managing the EMS certification process, providing materials to the EMS vendor, reviewing and responding to EMS vendor deliverables, participating in the System Testing effort and managing the User Acceptance Testing effort. A member of the SOS PMO will fill the responsibilities of the EMS Certification Manager (ECM) and Core Lead (CL) as detailed in section 2.1 and table 2 below.

SOS ITD – Application:

The SOS ITD – Application team is responsible for reviewing and responding to EMS vendor deliverables as indicated in section 2.1 (both during informal pre-submission reviews and deliverable review). Specifically, this team will fill the responsibilities of the Core Lead for the EMS System Code Delivery deliverables.

SOS ITD – Infrastructure:

The SOS ITD – Application team is responsible for reviewing and responding to EMS vendor deliverables as indicated in section 2.1 (both during informal pre-submission reviews and deliverable review). Specifically, this team will fill the responsibilities of the Core Lead for the EMS System Architecture Document deliverables.

SOS Risk Management Office:

The SOS Risk Management Office is responsible for reviewing and responding to EMS vendor deliverables as indicated in section 2.1 (both during informal pre-submission reviews and deliverable review). Specifically, this team will fill the responsibilities of the Core Lead for the Security deliverables.

SOS VoteCal Help desk:

The SOS VoteCal Help Desk is responsible for reviewing and responding to EMS vendor deliverables as indicated in section 2.1 (both during informal pre-submission reviews and deliverable review). Additionally, this team is responsible to provide VoteCal system help desk support throughout the EMS certification process including participation in Systems testing and User Acceptance Testing.

VoteCal Maintenance and Operations Contractor:

The VoteCal Maintenance and Operations Contractor is responsible for building VoteCal certification testing environments, smoke testing these environments, and managing/reporting on the execution of the System Testing effort, including review of EMS vendor’s System Test plan and Performance Test plan including test results. The VoteCal Maintenance and Operations Contractor will provide updated test cases and structure for use with System Testing including new or modified VoteCal functionality affecting the EMS. The VoteCal Maintenance and Operations Contractor will track System Test progress within Test Manager and report status on a bi-weekly basis during system testing. Additionally, the VoteCal Maintenance and Operations Contractor technical team will provide VoteCal system support when deemed necessary.

Counties:

Counties interested in supporting an EMS through certification are responsible for defining county requirements and outlining what an EMS vendor must provide to the county for the county to verify that the system meets their county requirements. Counties will be responsible to review Deliverables the EMS vendor provides and they are responsible to verify that the given EMS meets all county requirements. Counties will also be responsible to verify that data migration from their old EMS to their new EMS was successful and will actively participate in User Acceptance Testing to test data migration, and the ability of the EMS system to meet county and VoteCal integration requirements.

## Deliverable Review Responsibilities

The following deliverable review responsibility matrix shows which staff will be involved in the review process described below for each EMS deliverable throughout the certification process:

Table 1 – Deliverable Review Responsibilities

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **#** | **Deliverable / Task Name** | SOS PMO | | SOS VoteCal Help Desk | VoteCal M&O Contractor | County | SOS ITD - Infrastructure | SOS ITD - Application | SOS Risk Management Office |
| 1 | Initiation applications | ECM | DR |  |  |  |  |  |  |
| 2 | Software System Design Document | ECM | CL | DR |  | DR |  | DR |  |
| 3 | System Architecture Document | ECM | DR |  |  |  | CL | DR |  |
| 4 | Performance Test Plan | ECM | CL | DR | DR |  | DR | DR |  |
| 5 | Security Test Plan | ECM | DR |  | DR |  |  | DR | CL |
| 6 | System Test Plan | ECM | CL | DR | DR |  |  |  |  |
| 7 | EMS System Code delivery | ECM |  |  |  |  |  | CL |  |
| 8 | System, Performance, and Security Testing Results | ECM | CL | DR | DR (-Security) |  | DR | DR |  |
| 9 | User Acceptance Test Plan | ECM | CL | DR |  | DR |  |  |  |
| 10 | System Training Plan | ECM | DR | DR |  | CL |  |  |  |
| 11 | System User Manual | ECM | DR | DR |  | CL |  |  |  |
| 12 | County Migration Plan | ECM | DR | DR |  | CL |  |  |  |
| 13 | Final EMS Software Code | ECM |  |  |  |  |  | CL |  |
| 14 | Certification application | ECM | CL |  |  | DR |  |  |  |

Table 2 – Deliverable Review Roles

| Role | Responsibility |
| --- | --- |
| EMS Certification Manager | The EMS Certification Manager (ECM), in addition to having the responsibilities of a Deliverable Reviewer, is designated as responsible for consolidating and reviewing deliverable review comments from the review team to ensure they are comprehensive, clear, and concise. The ECM will evaluate the deliverable for adherence to the deliverable descriptions included within this EMS Certification plan and will identify and add any comments regarding gaps that are not already noted within the consolidated Comment Tracking Sheet (CTS). The ECM will also coordinate with SOS Subject Matter Experts (SMEs) (those that are not already listed as a Deliverable Reviewer for a given Deliverable), as required, to ensure completeness of SOS's review for a Deliverable. If needed, the ECM will facilitate a meeting with all Deliverable Reviewers, Subject Matter Experts (SMEs), and the EMS vendor to conduct walkthroughs and/or resolve any feedback discrepancies. In addition, the ECM will be responsible for making a recommendation and preparing the final Deliverable Response materials for approval and for providing them to the EMS organization after SOS approval. |
| Deliverable Reviewer | Deliverable Reviewers (DR) are members of the team who have been assigned responsibility for reviewing specific deliverables, documenting variances between deliverables under review, and the deliverable expectations included in the EMS Certification Plan. In addition, DRs are responsible to attend pre-submission walkthrough sessions and are responsible to review deliverables prior to these meetings whenever possible. DRs should actively participate in providing feedback in a clear and concise manner. During deliverable review, DRs may also identify possible deviations between the deliverable and SOS business or technical policy and may identify potential risks or issues which could negatively impact the successful implementation of the EMS with VoteCal. Any deviations between the deliverable and SOS business or technical policy should be documented in the comment tracking sheet and any risks or issues should be communicated to the ECM. Additionally, DRs are expected to collaboratively work with the Core Lead and/or the ECM to resolve questions and/or clarify deliverable feedback to the extent possible and within the timeframe prescribed. |
| Core Lead | The Core Lead (CL) will coordinate the collection of feedback for the deliverable among each DR, including from their own review and will be the first point of contact for questions from DRs and from EMS partners regarding the review. The Core Lead is also a DR for the given deliverable. The Core Lead will work to ensure that feedback from DRs is evaluated for consistency/appropriateness and that it is provided to the EMS partner. The Core Lead is responsible for verifying that the updated final version of the deliverables has addressed prior feedback provided and where these deliverables continue to be deficient the core lead is responsible for documenting the remaining deficiencies within the comment tracking sheet within the prescribed review timeframe. |

# Certification Process

Below are the EMS Certification phases an EMS vendor will follow to become certified in the state of California to interface with the VoteCal system:

The remaining sections detail each step in the process along with deliverables required to be approved to advance to the following phase. The SOS processes EMS certification applications on a “first come first served” basis. To this end the, and in-order to utilize SOS resources for the most benefit to the State of California, the SOS reserves the right to prioritize SOS resource time to those EMS vendors that have entered the Internal Development / Testing phase and as well place increased priority on those that enter the System Testing phase and subsequent phases.

## Initiation

In the Initiation Phase, introductory VoteCal materials will be provided to an interested EMS vendor, the vendor reviews these materials and can choose to complete an application to initiate the certification process. The SOS reviews the application and can provide formal approval to begin the certification process by signing the associated non-disclosure agreement.

### Introduction

If an EMS vendor expresses interest in becoming certified with the Secretary of State to operate in California and interface with the VoteCal system, the SOS will provide the following introduction materials to them so that they may evaluate what is required to become certified and determine if they wish to proceed. Below is a table of these introduction materials along with a description and their file names:

Table 3 – Introduction Materials

| Title | Description | File Name |
| --- | --- | --- |
| Introduction Email | Email to interested EMS vendors including all introduction materials including the EMS Certification Application form. | “Introduction Email.docx” |
| EMS Certification Application | This document provides detailed instructions for completion and submission of an EMS certification application. An application is considered complete only when all appropriate forms and supplemental materials are provided to the SOS. | “EMS Certification application\_dv1.0.pdf” |
| EMS Standard Values | Includes listing of the VoteCal data standards as of the last update to the data standards.  *Note: The VoteCal team plans to update these requirements again with each subsequent major VoteCal release.* | “VoteCal\_Standard\_Values\_Extract\_02082021.xlsx” |
| EMS Requirements | Requirements for the EMS to meet VoteCal integration specifications. These are requirements that the EMS must meet in-order to become certified as an EMS in the state of California. A summary sheet and two additional tabs are included, one for functional requirements and one for performance requirements.  Note: *The SOS has updated these requirements to include requirements covering all new and/or updated functionality since the implementation of VoteCal and up to March 2021.* | “vc-emsis-ems-requirements\_3-10-2021” |
| VoteCal Integration Service Catalog | Catalogs the VoteCal Integration services and includes short descriptions for each of the operations associated with each integration service.  Note: *The VoteCal team has updated the catalog in March 2021 to represent releases up and through February 2021.* | “vc-ems-intg-service-catalog\_3-10-2021.xlsx” |
| II.4 VoteCal System EMS Integration and Data Exchange Specifications | Main document of the EMS integration and data exchange specifications for VoteCal. VoteCal System EMS Integration and Data Exchange Specifications contains:   * Integration Specifications * Integration Service Rules * VoteCal Standard Code Values * EMS Requirements | “II.4-deliv-emsis-v6.0f-06292016.docx” |
| III.3 Acceptance Test Plan for Certification of EMS Data Integration and Compliance (CETP) | The VoteCal CETP describes activities conducted to test the integration of currently certified Election Management System (EMS) with VoteCal as specified by II.4 – VoteCal System EMS Integration and Data Exchange Specifications Document (EMSIS) and II.8 – VoteCal System Data Integration Plan (DIP). | “III.3-deliv-cetp-v1.4f-10162015.docx” |
| California Elections Code | The California Elections Code outlines the codes and regulations California election officials are responsible to adhere to. | Link: <http://leginfo.legislature.ca.gov/faces/codesTOCSelected.xhtml?tocCode=elec> |
| VoteCal Regulations | These regulations establish standards and procedures for processing, transmitting, and maintaining voter registration records in a manner that conforms with the statewide voter registration system requirements. | Link: <https://www.sos.ca.gov/administration/regulations/current-regulations> |
| Advisories to County Elections Officials | The California Secretary of State periodically provides written guidance and information to the state's county elections officials to help ensure a smooth electoral process.  The written advisories -- known as CCROVs since they are directed to county Clerks & Registrars of Voters -- are posted online shortly after they are provided to county elections officials. Electronic copies of all CCROVs dating back to January 2, 2007, are posted at the provided link.  EMS vendors can try searching for “VoteCal” or any other more specific topic for VoteCal related advisories in the “Search all Advisories” box. | Link: [County Elections Officials Advisories](https://www.sos.ca.gov/elections/advisories-county-elections-officials) |

If the EMS vendor chooses to proceed, they must complete the application to initiate the certification process and obtain SOS approval prior to SOS providing access to all the remaining certification materials to begin the Planning phase.

### Application to Initiate the Certification Process

The application form is composed of the following five parts and one additional appendix. The complete application to initiate the certification process must be completed and emailed, with scanned signature, to [VoteCalEMSCertification@SOS.CA.gov](mailto:VoteCalEMSCertification@SOS.CA.gov) to request initiation of the Planning phase. Please reference the application for the details:

* Part 1 – EMS System Identification and Non-Disclosure
* Part 2 – Ownership & Control
* Part 3 – References
* Part 4 – System Documentation Package – For The application to initiate the certification process the following additional materials should be submitted with the application:
  + Current System User Manual – Any documentation covering “how to” instructions for all EMS functionalities supplied to existing customers for use by the person(s) who are or will be using the system.
  + Current Software System Design Document – Any documentation describing the logical design of the software, the various modules of the software, their functions, and their interrelationships with each other. This includes the database design, input formats, output layouts, human-machine interfaces, and external interfaces.
  + Current System Architecture Document - Document describing the logical representation of the system, consisting of system components, hosting solutions, systems developed, communication paths and end points that work together to implement the overall system.
* Part 5 – Attestation and Signatures
* Appendix A: Non-Disclosure Agreement

Once the Application to initiate the certification process is received from the EMS vendor, the ECM will initiate and manage the evaluation of the EMS vendors application, including reviewing the application and providing updates to the VoteCal Director and EMS vendor. The evaluation process will include review by the VoteCal Director, and any other VoteCal staff the VoteCal Director deems appropriate. The VoteCal Director can then provide approval by signing the non-disclosure agreement included in the application.

## Planning

To start the Planning phase, the EMS Certification Manager will provide the SOS-approved application to initiate the certification process, to the EMS Vendor along with the additional VoteCal materials outlined below in Table 3. These materials are designed to, in combination with introduction materials introduced in the prior section, fully define the interface between VoteCal and the counties EMS, and provide the detail needed for EMS vendors to generate the required EMS certification deliverables and to remediate and/or develop their EMS application to conform to VoteCal standards. These materials will be updated at each subsequent major VoteCal release and be provide to all EMS vendors who have started this phase. Below is a listing of these materials along with a description of what they are used for and their filename:

Table 4 – EMS Certification Materials

| Title | Description | File Name |
| --- | --- | --- |
| Integration service documents | These are the Integration service design documents describing the various web services that allow communication between VoteCal and an EMS.  *Note: Integration service documents available are those current as of 2/2021.* | “VoteCal Integration Services\_3-12-2021.zip” |
| VoteCal Integration service rules | These are rules that dictate what validations VoteCal will impose for each of the Integration services and their operation’s fields.  *Note: VoteCal Integration service rules available are those current as of 2/2021.* | “VoteCal Integration Rules\_3-12-2021.zip” |
| Interface Design Description | The interface design defines the functional design of an exchange of information between VoteCal and other systems. This document provides detail about both inbound and outbound file structure, fields, validation as well as error handling and process logging.  *Note: VoteCal Integration service rules available are those current as of 4/2020.* | “II.3-dsd-idd\_4-2020.docx” |
| Common Contracts documentation | This document is a service design document describing the data and fault contracts used across all layers of the VoteCal system, including components that integration with EMSs.  *Note: VoteCal Common Contracts available are those current as of 2/2021.* | “vc-common-contracts\_3-12-2021.docx” |
| Synchronization Hash Specs | This describes the process of using hashes to perform synchronization checks between VoteCal and the county implementation of the EMS. | “vc-synchronization-hash-specs\_3-12-2021.xlsx” |
| VoteCal dynamic link library (DLL) files | VoteCal DLLs are files that allow EMS vendors to create XML schema definition (XSD) for the 62 messages/payloads used for EMS inbound/outbound Messaging. These DLLs are provided to facilitate development of the EMS interface to VoteCal prior to the availability of a connection to a VoteCal test environment.  *Note: VoteCal DLLs available are those current as of 2/2021.* | “VoteCal DLLs For EMS\_2.6.13.5\_3-2-2021.zip” |
| System Test Case Summary | This is a summary of system test cases that must be passed for the EMS to attain certification.  *Note: The SOS intends to supplement the existing test cases with system test cases coving new and/or updated functionality since the implementation of VoteCal prior to execution of system testing.* | “VoteCal System Test Scenario Summary.xlsx” |

The EMS vendor must complete the following deliverables/steps, and obtain SOS approval, before the planning phase can be considered complete:

* Product Demo
* Deliverable 1: *Interim* Work Breakdown Structure
* Deliverable 2: *Interim* Software System Design Document
* Deliverable 3: *Interim* System Architecture Document
* Deliverable 4: *Interim* Performance Test Plan
* Deliverable 5: *Interim* Security Test Plan
* Deliverable 6: *Interim* System Test Plan
* Deliverable 7: *Interim* EMS Code Delivery

The remaining sub-sections below detail SOS’s expectations for each of these deliverables at this phase of the project.

### Deliverable 1: Work Breakdown Structure

The Work Breakdown Structure (WBS) is expected to describe a deliverable-oriented hierarchical decomposition of the work to be executed by the project team to accomplish the project objectives and create the required deliverables. The WBS is used for effective project planning, execution, controlling, monitoring, and reporting. All the work contained within the WBS is to be identified, estimated, scheduled, and budgeted.

### Deliverable 2: Interim Software System Design Document

The System Design Document is expected to describe:

* system requirements,
* operating environment,
* files and database design,
* input formats,
* output layouts,
* human-machine interfaces,
* detailed design,
* processing logic, and
* external interfaces for the EMS

This documentation should also clearly indicate the various modules of the software, their functions, and their interrelationships with each other. At the end of the Planning phase the Software System Design Document must show coverage of at least **33%** of the EMS Requirements. The Deliverable should include a mapping from EMS requirement to the pages and/or sections in the design document where the requirement is covered. Coverage should include screenshots, data structures, VoteCal integration services, and data field level specifications to be used to meet the requirements. References to the Common Contracts document can be leveraged to provide field level specifications for the Software System Design Document provided one, the EMS vendor has mapped the specific data contracts and field level specifications within the Common Contracts document to the data fields included in the design document and two, the specifications for these fields within the EMS are identical to VoteCal as documented in the Common Contracts document.

### Deliverable 3: System Architecture Document

The System Architecture Document is a conceptual model that defines the structure and behavior of the EMS system. The document should describe the EMS application’s various modules and components, the relationships among those modules and components, and the [rules](https://en.wiktionary.org/wiki/rule) governing those relationships. The architecture components described should consist of EMS hardware, [software](https://en.wikipedia.org/wiki/Software), documentation, facilities, manual procedures, system roles and interface(s) between the VoteCal system, other external interfaces, and its [user](https://en.wikipedia.org/wiki/User_(computing))s.

The System Architecture Document is expected to describe the logical representation of the system, consisting of system components, systems developed, communication paths and end points, that work together to implement the overall Election Management System. Below is an example document outline:

* Introduction
* Methodology
* Logical Design
* Technical Design
  + Presentation Layer
  + Service Layer
    - Integration Services
    - Business Services
    - Common Services
    - Technical Services
    - Security Services
  + Information Layer
    - Data Services
      * Object to Relational Mapping Framework
    - Transactional Data Model
    - Non-Structured and Document Storage
    - Reporting
  + Integration Layer
    - Integration Design Patterns
    - Service Bus Framework
    - EMS to SOS VoteCal Message Transformations
    - SOS VoteCal Replies
      * SOS VoteCal Payload to EMS Message Transformation
      * Reply Message Processing
      * Error Processing
        + Logging

### Deliverable 4: Performance Test Plan

The performance test plan is expected to describe the testing that will be completed to ensure that the EMS will function uninterrupted and efficiently under periods of high usage (typically coinciding with a California election). The types of performance testing that should be addressed are as follows:

* Load testing – A test of multiple users or test process emulating peak demands.
* Stress testing – Going beyond system limitations to identify actual limitations.
* Endurance testing – Test a high volume for an extended period of time.
* Resilience testing – Test loss of connectivity and service disruption.
* Recovery testing – Test how the system recovers following crashes and/or HW failures.

The Performance Test Plan should also include a listing of all the performance requirements, listed below and/or agreed to between the SOS and the EMS vendor, along with the testing approach that will be followed to ensure that all these requirements are met.

Performance test cases and test results are not required at this point in the process. Performance test cases will be required at the completion of the Internal Development / Testing phase and performance test results will be required at the end of the System Testing phase.

The performance requirements that must, at a minimum, be included and covered by the planned performance testing approach are as follows:

Table 5 – Performance Requirements

|  |  |
| --- | --- |
| **Requirement #** | **Requirement Description** |
| P1 | The EMS must support and maintain fifteen hundred (1500) concurrent users at a time for a county (e.g. L.A.). |
| P2 | After the receipt of the Official List from VoteCal, The EMS must support processing VoteCal Official List (i.e. Compare county and VoteCal data, determine differences, and reason) at the rate of one million (1,000,000) records every 10 minutes for a county (e.g. L.A.). |
| P3 | The EMS must support the following sustained transaction volumes concurrently for a county (e.g. L.A.): • One hundred (100) county transactions (e.g., data transmittal of new and updated voter registration data, search for existing records, statewide data retrieval for a record) every one minute; • Receive 100 hundred (100) electronic notifications such as New Voter, Resolve UID, DMV Voter Registration every one minute; |
| P4 | The EMS must support six million (6,000,000) voter records as implemented for a county (e.g. LA). The EMS must be able to scale to ten million (10,000,000) voter records with the addition of hardware, operating system and third party software licenses only for a county (e.g. L.A.) |
| P5 | The EMS must provide the capacity to store an average of ten (10) affidavit images and ten (10) signature images for each voter for a county (e.g. L.A.). |
| P6 | The EMS system must automatically process at a rate of less than one minute per California Online Voter Registrations (COVR) transactions from the time the transaction is received at EMS queue. Processing of the transaction includes validation checks, address correction, precincting, and so on. |
| P7 | As the recipient of electronic notification to send county data for Synchronization Check, The EMS must send to VoteCal the hash values of Voter and District & Precinct at the rate of one million (1,000,000) records every five (5) minutes. |
| P8 | At the receipt of Synchronization result, The EMS must process (i.e. compare VoteCal with county data, determine different, and reason) result at the rate one million (1,000,000) records every five (5) minutes. |
| P9 | The EMS system send to VoteCal concurrently one thousand (1000) district-precinct mapping continuously in 5 minutes. |
| P10 | The EMS system send to VoteCal concurrently five hundred thousand (500,000) voter participation, vbm ballots, and provisional ballots continuously in fifteen (15) minutes. |
| P11 | For local EMS searches using exact-match criteria on two (2) or more individually identifying data attributes (e.g., combination of Last Name, Data of Birth, First Name) The EMS must return results within the following time frames:  • 90% of the searches complete in less than one (1) second; • 98% of the searches complete in less than two (2) seconds; and • 100% of searches complete in less than (5) seconds. Note: Local EMS search only looks at county records. |
| P12 | The EMS must allow the county to back up EMS data and configurations for all EMS county components on periodic basis. |
| P13 | The EMS must provide the ability to restore data, systems, and/or county configurations of the counties EMS from a backup within a mutually agreeable timeframe between the county, SOS, and EMS vendor. |
| P14 | When network connectivity to VoteCal is down or the VoteCal application is unavailable the EMS application must continue to operate with minimal impacts to the end user outside those that require direct connectivity to VoteCal. Once VoteCal is and/or connectivity is available the EMS should be able to resume processing EMS messages and, transactions that have been queued during these time periods. |
| P15 | If the EMS application becomes unavailable it should later be able to resume processing EMS messages and transactions that have been queued, once the EMS application is again available. |
| P16 | The EMS must provide transactional integrity for data and must be able to report back when a transaction fails. |
| P17 | The EMS must maintain an SLA of 99.95% uptime or as otherwise mutually agreed to by impacted counties, the SOS and the EMS vendor. |

### Deliverable 5: Security Test Plan

The SOS expects that the Security test plan be developed to specifically address each of items included within the VoteCal Draft Regulations document, section “19064. County Security” included below. Detailed descriptions of the security approach that the EMS’s vendor will have in place to enable the county to meet each of these regulations is expected to be described in detail. Security Test Cases are not required at this point in the process but will be required at the completion of the Internal Development / Testing phase. Additionally, security test results will be required at the completion of the System Testing phase.

Table 6 – County Security Requirements

|  |
| --- |
| 19064. County Security  1. Each county shall protect the confidentiality, integrity, and availability of the data and the election information system authorized to process, store, and transmit voter registration data. This system shall utilize system hardening and resilient architecture by means of redundancy, high availability, or other fault-tolerant methodologies. 2. Each county shall provide annual privacy and security awareness training to all staff and contractors, if any, utilizing its county voter registration and election information system in accordance with State Administrative Manual sections 5320 – 5320.2 and the Information Practices Act of 1977 (Civil Code section 1798, et seq.). 3. Each county shall complete a security assessment of its election information system prior to a statewide primary election. The security assessment shall evaluate the: 4. Active management (inventory, tracking, and correction) of all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access. 5. Active management (inventory, tracking, and correction) of all software on the network so that only authorized software is installed and can execute, and unauthorized and unmanaged software is found and prevented from installation or execution. 6. Establishment, implementation, and active management (tracking, reporting, and correction) of the security configuration of laptops, servers, and workstations in order to prevent attackers from exploiting vulnerable services and settings. 7. Continuous acquisition, assessment, and action on new threats in order to identify vulnerabilities, and to remediate and minimize opportunity for attacks. 8. Tracking, control, prevention, and correction of the use, assignment, and configuration of administrative privileges on computers, networks, and applications. 9. Collection, active management, and analysis of audit logs of events that could help detect, understand, or recover from an attack. 10. Minimization of opportunities for attackers to manipulate human behavior through their interaction with web browsers and e-mail systems. 11. Control of the installation, spread, and execution of malicious code at multiple points in the election information system, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action. 12. Active management (tracking, control, and correction) of the ongoing operational use of ports, protocols, and services on networked devices in order to minimize vulnerabilities available for attack. 13. Proper backup of critical data to allow for timely recovery. Backups shall be made at least every 24 hours. Backups for counties with more than 50,000 registered voters as of the last Report of Registration are recommended more frequently. Each county shall review critical data backup and recovery procedures to ensure the backups are not stored on the same servers hosting the county voter registration and election information system, and that restoration procedures are detailed and complete. 14. Establishment, implementation, and active management (tracking, reporting, and correction) of the security configuration of network infrastructure devices in order to prevent attacks exploiting vulnerable services and settings. 15. Detection, prevention, and correction of the flow of information transferring between networks of different trust levels with a focus on security-damaging data. 16. Prevention of data exfiltration, mitigating the effects of exfiltrated data, and ensuring the privacy and integrity of sensitive information. 17. Tracking, controlling, preventing, correcting, and securing access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets. 18. Tracking, controlling, preventing, and correcting the security use of wireless local area networks, access points, and wireless client systems. 19. Active management of the life-cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them. 20. Identification of the specific knowledge, skills, and abilities needed to support defense of the election information system; development and execution of an integrated plan to assess, identify and remediate gaps, through policy, organizational planning, training, and awareness programs for all functional roles in the organization. 21. Active management of the security life-cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses. 22. Protection of the organization’s information, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, and management oversight). 23. Testing of the overall strength of an organization’s defenses (technology, processes, and people) by simulating the objectives and actions of an attacker. 24. Each county and its EMS vendor shall take the following security measures to provide security for the county’s EMS and election information system, as well as for environments that interface with the statewide voter registration system and/or contain statewide voter registration system data: 25. At all times servers hosting county voter registration and election information systems including the county’s EMS as well as any Secretary of State property, such as routers, shall be secured in a designated area away from public access. The designated area shall be secured with a method to determine the identity of each person that has accessed the designated area and unauthorized access to this designated area must be detectable. 26. Only staff authorized by the county shall have physical access to servers hosting the county’s EMS and election information system, including servers containing the county’s EMS as well as any Secretary of State property, such as routers. 27. The county’s EMS and election information system shall only be accessible by persons authorized by the county. 28. No peripheral devices (e.g., disks, flash drives, smartphones, etc.) shall be attached to Secretary of State property, such as routers, installed at the county. 29. Secretary of State property, such as routers, installed at the county shall be exclusively for interaction with the Secretary of State, and shall not to be used for other county purposes. 30. The servers hosting the county EMS and election information system shall be running an operating system under mainstream support with critical and high security patches and updates applied at least monthly. All servers shall otherwise be hardened to industry best practices and government standards. 31. The county’s EMS and election information system shall be installed and operated on a service account separate from any other services. 32. The county’s EMS and election information system shall have anti-malware software installed and configured, and updates regularly applied. 33. Counties shall encrypt all voter registration and election information system data whenever stored in non-volatile memory and whenever in transit between system components or through facilities not contracted directly to the county or the Secretary of State. 34. All backup copies of county voter registration and election information system data, including images, shall be encrypted. Counties shall avoid the use of removable, portable media such as tape cartridges or DVD/ROM for data backup unless approved in writing by the Secretary of State based on the unique circumstances of the county, such as its information technology resources. 35. Data encryption shall be compliant with National Institute of Standards and Technology Special Publication 800-175B, Guideline for Using Cryptographic Standards in the Federal Government, with preferred utilization of Advanced Encryption Standard (published August, 2016; incorporated by reference). However, effective July 1, 2021, the county and its EMS vendor shall use Federal Information Processing Standards Publication 140-2 (FIPS 140-2) for data encryption for the county’s EMS and election information system, as well as for environments that interface with the statewide voter registration system and/or contain statewide voter registration system data (Published May 25, 2001; incorporated by reference). 36. Direct user access to the county’s EMS and election information system shall require, at a minimum, single sign-on authentication. However, effective July 1, 2021, direct user access to the county’s EMS and election information system shall require, at a minimum, two (2) sign-on authentications. 37. The county’s EMS and election information system shall implement security log management, which includes the following: 38. Log all systems and network devices with sufficient information collection. 39. Securely store log files separately from the systems monitored, keep these files archived, and protect these files from unauthorized modification, access, or destruction. 40. Use log monitoring tools to send real-time alerts and notifications. 41. Utilize multiple synchronized United States-based time sources. 42. Counties shall regularly review log(s) for any errors, abnormal activities, and any system configuration changes. 43. Counties shall report detected unauthorized use, suspected breach, or denial of service attack on the county’s EMS and election information system to the Secretary of State Elections Division Help Desk within 24 hours of discovery. |

### Deliverable 6: System Test Plan

The System Test Plan (STP) should describe the way the EMS vendor intends to conduct and complete testing of the EMS Application with VoteCal system and other EMS interfacing partners to meet:

* The specifications in II.4 – VoteCal System EMS Integration and Data Exchange Specifications Document (EMSIS),
* County requirements and
* State requirements.

The purpose of this test is to evaluate the system's compliance with county and state requirements and the ability of the EMS to interface with VoteCal to exercise all integration services and their operations. The EMS’s System Test Plan, at the Planning phase, is expected to (per IEEE 829 standards) describe the approach the EMS vendor will take to address the following:

* Resumption/Suspension of testing criteria.
* Test deliverables - test cases, test scripts, defect logs, test reports and test environment to be used.
* Test environment set up requirements.
* Training and staffing.
* EMS vendor Team member responsibilities.
* Testing Schedule.
* Planning for Risks and Contingency Plans.
* Exit Criteria and Approvals required.

A complete listing of system test cases is not expected during the Planning phase but will be provided as part of the Internal Development / Testing phase. Similarly, system test results will not be required during the Planning phase but will be expected at the completion of the System Testing phase.

### Deliverable 7: Interim EMS Code Delivery Expectations

EMS software code representing the version being submitted for this phase, including all county installation and setup instructions/requirements are required to be submitted and reviewed by the SOS.

The SOS will use SonarQube to evaluate the vendors’ UI and Server codebase. Veracode will be used for application security testing to conduct a vulnerability scan of the code.

SonarQube has a free community version that takes a reasonable amount of effort for initial set up and configuration, about a day. It is strongly suggested that the vendors configure SonarQube in their own environment and validate their code against these expectations prior to submission of the code deliverable.

* Per SonarQube:
  + The code will have 0 bugs,
  + The code will have 0 Security Vulnerabilities,
  + Automated testing will have at least 90% code coverage, and
  + Codebase will have less than 5% Duplicated Code.
* Per Veracode:
  + No critical or high issues should exist and all medium bugs shall be mitigated (Minimum Veracode  level: VL5+SCA with 90 minimum score).

If any of the above criteria are not met, then the EMS vendor will provide an explanation for each not-met item. For example, if the codebase is evaluated to have 10% Duplicated Code, a write up should be attached that explains why the Duplicate Code is at 10% instead of 5% and what is preventing the Duplicate Code from being reduced to 5%.

For SOS to do the internal source code evaluation a valid DEBUG build environment must be provided.

Ways a vendor can provide a valid DEBUG build environment are as follows:

* Provide a plug and play deployable container that can be set up locally at SOS.
* Provide source code along with instructions on how to set up a local build environment.

Discussions between SOS and the vendor may be required to complete the required setup.

## Internal Development / Testing

Once the planning phase has completed (all required Deliverables have been approved) the EMS vendor will be granted permissions to start the Internal Development / Testing phase and be provided with connection credentials to connect with a dedicated VoteCal test sandbox environment. The EMS vendor will have up to 6 months access to this dedicated VoteCal sandbox test environment to complete code development and any internal testing with VoteCal. It is expected that within this phase the EMS vendor will fully develop all integration components with VoteCal and will be ready to pass all system tests. It is also expected that EMS vendors will work with and select a pilot county and that this county has expressed their intention to migrate to the given EMS vendor. This can be communicated to the SOS by the county ROV or designated staff with the authority to make this decision.

Below are the SOS-ITD technical connection requirements EMS vendors at this stage will need to meet:

Table 7 – Technical SOS-ITD connection requirements

|  |
| --- |
| 1. Network device must support site to site VPN 2. Network device must support IPSec in tunnel mode and at minimum IKEv1. It is strongly recommended to use IKEv2. If using IKEv1, the only exchange mode supported for IKE negotiation is Main Mode 3. Network device must support any of the following IKE crypto policies (from strongest to weakest):    1. DH Group—group20, group19, group14.    2. Authentication—sha512, sha384, sha256.    3. Encryption—aes-256-cbc, aes-192-cbc, aes-128-cbc.    4. IKE SA Lifetime – Maximum 24 hours (86400 seconds), unless otherwise stated. 4. Network device must support any of the following IPSec Crypto policies (from strongest to weakest):    1. Protocol – ESP (Encapsulating Security Payload) only.    2. Encryption—aes-256-gcm, aes-256-cbc, aes-192-cbc, aes-128-gcm, aes-128-ccm, aes-128-cbc.    3. Authentication—sha512, sha384, sha256.    4. SA Phase 2 - group20, group19, group14.    5. IPSec/Child SA Lifetime – Maximum 8 hours (28800 seconds), unless otherwise stated. 5. A technical staff member will be required to validate that the VPN tunnel is connecting and working as intended. This staff member will also facilitate any troubleshooting that may be required. 6. An interconnect agreement shall be established. |

To complete the Internal Development / Testing phase, the EMS vendor must deliver, and the SOS must approve the following deliverables:

* Deliverable 2: *Interim* Software System Design Document
* Deliverable 3: System Architecture Document
* Deliverable 5: *Interim* Security Test Plan
* Deliverable 6: *Interim* System Test Plan
* Deliverable 7: *Interim* EMS Code delivery

Deliverables in this phase will be broken down into two stages as indicated below.

Internal Development and testing, Stage 1:

Once the vendor validates completion of testing with VoteCal integration services, and SOS approves the following deliverables, the SOS will provide the EMS with a repository to all system test scripts (Only VoteCal side steps will be detailed out) that must be passed in the System Testing phase:

* Deliverable 2: Software System Design Document
* Deliverable 3: System Architecture Document
* Deliverable 7: Interim EMS Code delivery

Internal Development and testing, Stage 2:

To demonstrate the completion of Internal Testing the EMS must submit the remaining deliverables indicated below:

* Deliverable 2: Software System Design Document
* Deliverable 5: Security Test Plan
* Deliverable 6: System Test Plan
* Deliverable 7: Interim EMS Code delivery

The remaining subsections describe the specific expectations for these Deliverables at this phase of certification.

### Deliverable 2: Software System Design Document

It is expected that at this phase the EMS software is developed and tested internally by the EMS vendor and that a complete and current design addressing all security, performance, system and county requirements is provided. The System Design Document is expected to describe:

* system requirements,
* operating environment,
* files and database design,
* input formats,
* output layouts,
* human-machine interfaces,
* detailed design,
* processing logic, and
* external interfaces for the EMS.

This documentation should also clearly indicate the various modules of the software, their functions, and their interrelationships with each other.

At the end of stage 1 of the Internal development and testing phase the Software System Design Document must show coverage of all EMS Requirements. The Deliverable should include a mapping from EMS requirement to the pages and/or sections in the design document where the requirement is covered. Coverage should include screenshots, data structures, VoteCal integration services, and data field level specifications to be used to meet the requirements. References to the Common Contracts document can be leveraged to provide field level specifications for the Software System Design Document provided one; the EMS vendor has mapped the specific data contracts and field level specifications within the common contracts document to the data fields included in the design document and two; the specifications for these fields within the EMS are identical to VoteCal as documented in the common contracts document.

At the end of stage 2 of the Internal development and testing phase the Software System Design Document must have all design findings discovered while in this phase incorporated into the document for re-submission.

### Deliverable 3: System Architecture Document

It is expected that at this phase the System Architecture Document is updated to reflect any modifications or updates that were introduced during the internal development and testing phase.

The System Architecture Document is a conceptual model that defines the structure and behavior of the EMS system. The document should describe the EMS application’s various modules and components, the relationships among those modules and components, and the [rules](https://en.wiktionary.org/wiki/rule) governing those relationships. The architecture components described should consist of EMS hardware, [software](https://en.wikipedia.org/wiki/Software), documentation, facilities, manual procedures, system roles and interface(s) between the VoteCal system, other external interfaces, and its [users](https://en.wikipedia.org/wiki/User_(computing)).

The System Architecture Document is expected to describe the logical representation of the system, consisting of system components, systems developed, communication paths and end points, that work together to implement the overall Election Management System. Below is an example document outline:

* Introduction
* Methodology
* Logical Design
* Technical Design
  + Presentation Layer
  + Service Layer
    - Integration Services
    - Business Services
    - Common Services
    - Technical Services
    - Security Services
  + Information Layer
    - Data Services
      * Object to Relational Mapping Framework
    - Transactional Data Model
    - Non-Structured and Document Storage
    - Reporting
  + Integration Layer
    - Integration Design Patterns
    - Service Bus Framework
    - EMS to SOS VoteCal Message Transformations
    - SOS VoteCal Replies
      * SOS VoteCal Payload to EMS Message Transformation
      * Reply Message Processing
      * Error Processing
        + Logging

### Deliverable 5: Security Test Plan

Security tests with detailed instructions, including tools to be utilized, actions taken and expected results describing the steps to verify security per the draft VoteCal regulations is expected at this phase of the certification. The complete collection of tests shall cover all of the county security requirements included in section “20112. County Security” subsection (d) of the draft VoteCal regulations.

### Deliverable 6: System Test Plan

The System Test plan, at this phase of the project, should include test scripts with detailed EMS instructions, including actions and expected results, describing steps to carry out all EMS functionality.

The SOS will provide the base set of test cases (leveraged from the VoteCal project’s III.3 – Acceptance Test Plan for Certification of EMS Data Integration and Compliance deliverable, VoteCal Project CETP test cases) in stage 2 of this phase. All these tests must be passed as tested internally as part of this phase.

The complete collection of test scripts that will be utilized will cover all VoteCal’s EMS specifications and standards, such that execution of all test scripts will verify that all requirements for the remediated EMS have been met. Each test script will include a reference to the requirement(s) and/or specification(s) which it is designed to test to establish traceability from requirements to specifications to test scripts. SOS expects test scripts to be comprehensive in their coverage of EMS requirements.

Additionally, the system test plan must include a mapping from the VoteCal Integration Service Catalog (Integration services and their operations) to the associated test that will test each of the integration services and their various operations.

Testing results from the EMS vendor’s internal testing is required to be included within the deliverable and these tests and results must be mapped to EMS requirements, Integration Services and their operations per the Integration Service Catalog. Internal test results are expected to show coverage of all integration services and their operations.

### Deliverable 7: Interim EMS Code delivery

The SOS expects that the EMS vendor submit the latest version of the EMS code, representing the EMS code base that will be used to start the System Testing phase. The SOS will review the code using the process outlined in section 3.2.7.

## System Testing

The System Testing phase will be used to test the integration between VoteCal and the EMS to verify that all VoteCal-EMS integration services and all their various operations are tested and verified as working as designed.

To complete the system testing phase the EMS vendor must deliver, and the SOS must approve, updated versions of the following deliverables:

* Deliverable 2: Software System Design Document.
* Deliverable 8: System, Performance, and Security Testing Results
  1. Deliverable 4: Performance Test Plan with results passing.
  2. Deliverable 5: Security Test Plan with results passing.
  3. Deliverable 6: System Test Plan with results passing.
* Deliverable 7: *Interim* EMS Code delivery.

### Execute System Testing

System testing will include up to two rounds of testing in which the EMS vendor will have the opportunity to pass. To pass, no severity two bugs shall exist, and the EMS vendor shall provide a mutually agreeable resolution plan for severity 3 or 4 bugs provided a feasible workaround exists.

The EMS vendor will be given one opportunity to resolve all identified bugs following the first round of execution of all system test cases, in the event the EMS vendor does not pass in the first round. The retest will include one additional run through all system tests and integration services as needed. If the retest does not resolve all Severity 1 and 2 reported defects, the resulting System Test Plan with results will not be accepted by the SOS and the EMS vendor and SOS will need to mutually agree on next steps.

The developed EMS vendor System Test Plan together with SOS provided system test cases (leveraged from VoteCal’s III.3 – Acceptance Test Plan for Certification of EMS Data Integration and Compliance) will make up the set of scenarios that will be executed during the System Test phase. These tests will be verified to cover all county and SOS requirements, VoteCal integration services and operations. The SOS, based on review of the EMS vendor Deliverables submitted in this phase, will decide if the EMS vendor has passed or not.

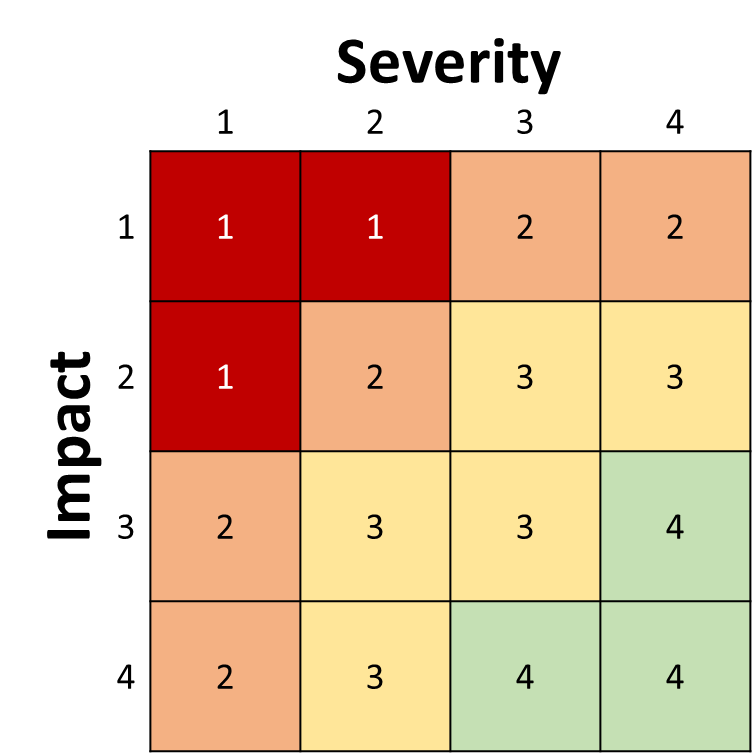
Defect severity is an assessment of the business consequence of a defect. The below table will be used by SOS and the EMS vendor to determine the severity of each defect identified during system testing.

Table 8 – System Testing Defect Severity Definitions

|  |  |
| --- | --- |
| Value | Severity |
| 1-Critical | * Prevents the accomplishment of an Essential Function.[[1]](#footnote-2) * Jeopardizes safety, security, or causes unrecoverable data loss. * No work around solution is known. |
| 2-High | * Adversely affects the accomplishment of an essential function and no known work-around solution. * Causes recoverable data loss but with high impact to users. * Impacts reliability of public-facing functionality or data. |
| 3-Medium | * Adversely affects the accomplishment of an essential function and a workaround solution is known or adversely affects the accomplishment of VoteCal functions. * Causes recoverable data loss |
| 4-Low | * Results in user/operator inconvenience or annoyance but does not affect a required operation or mission essential function. * Cosmetic or documentation issue to non-public facing functionality. |

Defect Priority is a value from 1 to 4, giving equal weighting to both Impact and Severity. The below matrix provides a consistent, objective way to set the initial priority based on impact and severity of the defect.

Figure 1 – Defect Prioritization



Priority is used by the EMS vendor as a guideline for assigning resources to fix defects and can be adjusted by mutual agreement with the SOS.

The remaining sub-sections describe the specific expectations for EMS Deliverables to complete the System Testing phase.

### Deliverable 2: Interim Software System Design Document

It is expected that at this phase the EMS software is fully developed by the EMS vendor and system tested by SOS and that a complete and current design addressing all security, performance, system and county requirements and test findings is provided. The Software System Design document sections covering each requirement should be updated to address all bugs and defects identified and/or resolved through system, performance, and security testing.

### Deliverable 8: System, Performance, and Security Testing Results

This Deliverable will consist of a consolidation of the below three.

#### Deliverable 4: Performance Test Plan with Results Passing

It is expected that at this phase the Performance Test Plan will be submitted with all results recorded and passing.

The Performance Test Plan shall include descriptions of all the performance (ex: load/volume) related testing that has been conducted on the remediated EMS in-order to verify that performance requirements have been met. Performance test results shall be provided including:

* Pass / fail percentages for all test executed,
* Descriptions of all deficiencies identified and/or resolved, and
* Confirmation of successful completion of the given test effort.

#### Deliverable 5: Final Security Test Plan with Results Passing

It is expected that at this phase the Security Test plan will be submitted with all results recorded and passing.

The Security Test Plan shall include descriptions of all the security related testing that has been conducted, including full source code review and penetration testing, on the remediated EMS in-order to verify that security requirements and drafted security regulations have been met. Security Test results shall be provided including:

* Pass / fail percentages for all test executed,
* Descriptions of all deficiencies identified and/or resolved, and
* Confirmation of successful completion of the given test effort.

#### Deliverable 6: Final System Test Plan with Results Passing

At this phase, the System Test Plan must include the results of the system testing effort and an updated mapping from the VoteCal Integration Service Catalog (Integration services and their operations) to the associated test. Test results must confirm successful verification of each of the EMS requirements, integration services and their various operations. Additionally, System Test results shall be provided including:

* Pass / fail percentages for all test executed,
* Descriptions of all deficiencies identified and/or resolved, and
* Confirmation of successful completion of the given test effort.

### Deliverable 7: Interim EMS Code delivery

The SOS expects that the EMS vendor submit the latest version of the EMS code, representing the EMS code base that will be used to start the User Acceptance Testing phase. The SOS will review the code using the process outlined in section 3.2.7.

## User Acceptance Testing

The EMS vendor must submit the following deliverables prior to completing the User Acceptance Test phase and/or obtaining conditional acceptance for certification:

* Execute UAT
* Deliverable 2: Software System Design Document
* Deliverable 3: System Architecture Document
* Deliverable 4: Performance Test Plan
* Deliverable 7: EMS Code Delivery
* Deliverable 9: User Acceptance Test Plan

The SOS, EMS vendor and the pilot county must also execute UAT and pass UAT exit criteria defined by the SOS and the county within the User Acceptance Test Plan.

All deliverables must be approved by the SOS and/or the pilot county and shall be submitted along with the final application to become certified. Please see below for details on the UAT phase and the deliverables required in this phase.

### Execute UAT

User Acceptance Testing will be generally based on conducting a mock election using the EMS with migrated county production data.  It is expected that the UAT will cover all County specific requirements as well as VoteCal Integration Requirements including, but not limited to the following processes and procedures related to an election:

* Election Setup and Creation, ROR, Official List, etc.
* Voter Registration, Duplicate Voter Matching
* Ballot Processing and Voter Participation History
* List Maintenance
* Synchronization
* County Specified Functionality

It is expected that the EMS vendor will be able to migrate production data from the pilot county’s current EMS to the UAT testing environment. It is mandatory that the EMS vendor and county rehearse and test the data migration process multiple times prior to migrating data for the purposes of UAT. The County Migration Plan, to be submitted in the subsequent phase will outline all the steps take to complete migration for the county including verification of success.

During UAT execution, the County and the SOS, depending on the test case step, will be responsible for recording test case step pass/fail results and will record any roadblocks or issues experienced.  Any issues or roadblocks will also be emailed to [VoteCalHelp@SOS.ca.gov](mailto:VoteCalHelp@SOS.ca.gov) as well as the EMS vendor help desk.  Tickets will be logged by the EMS vendor and the SOS VoteCal Help desk and a cross reference added to tie the tickets together.  The SOS will follow the production help desk processes and procedures to manage and resolve tickets and tickets will be logged as “UAT” tickets. A daily ticket triage call will be held by the SOS and EMS vendor as needed.

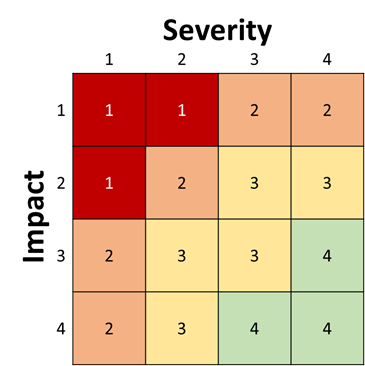
Tickets that result in identified bugs will be logged by the EMS vendor or the VoteCal team depending on the source of the problem. The below table will be used by SOS and the EMS vendor to determine the severity of each defect identified during UAT:

Table 9 – User Acceptance Testing Defect Severity Definitions

|  |  |
| --- | --- |
| Value | Severity |
| 1-Critical | * Prevents the accomplishment of an Essential Function.[[2]](#footnote-3)[1] * Jeopardizes safety, security, or causes unrecoverable data loss. * No work around solution is known. |
| 2-High | * Adversely affects the accomplishment of an essential function and no known work-around solution. * Causes recoverable data loss but with high impact to users. * Impacts reliability of public-facing functionality or data. |
| 3-Medium | * Adversely affects the accomplishment of an essential function and a workaround solution is known or adversely affects the accomplishment of VoteCal functions. * Causes recoverable data loss |
| 4-Low | * Results in user/operator inconvenience or annoyance but does not affect a required operation or mission essential function. * Cosmetic or documentation issue to non-public facing functionality. |

Defect priority is a value from 1 to 4, giving equal weighting to both impact and severity. The below matrix provides a consistent, objective way to set the initial priority based on impact and severity of the defect.

Figure 1 – Defect Prioritization



UAT results will be compiled and shared by the SOS daily and will include:

* Pass / fail percentages for all test executed,
* Descriptions of all deficiencies identified and/or resolved, and

To pass UAT, all tests must be executed, no severity one or two bugs shall exist, and the EMS vendor shall provide a mutually agreeable resolution plan for severity 3 or 4 bugs provided a feasible workaround exists.

### Deliverable 2: Final Software System Design Document

It is expected that at this phase the EMS software is fully developed by the EMS vendor and that a complete and current design addressing all security, performance, system and county requirements and test findings is provided. The Software System Design document sections covering each requirement should be updated to address all bugs and defects identified and/or resolved through UAT, system, performance, and security testing.

### Deliverable 3: Final System Architecture Document

It is expected that at this phase the System Architecture Document is updated to reflect any modifications or updates that were introduced during the UAT phase.

The System Architecture Document is a conceptual model that defines the structure and behavior of the EMS system. The document should describe the EMS application’s various modules and components, the relationships among those modules and components, and the [rules](https://en.wiktionary.org/wiki/rule) governing those relationships. The architecture components described should consist of EMS hardware, [software](https://en.wikipedia.org/wiki/Software), documentation, facilities, manual procedures, system roles and interface(s) between the VoteCal system, other external interfaces, and its [user](https://en.wikipedia.org/wiki/User_(computing))s.

The System Architecture Document is expected to describe the logical representation of the system, consisting of system components, systems developed, communication paths and end points, that work together to implement the overall Election Management System. Below is an example document outline:

* Introduction
* Methodology
* Logical Design
* Technical Design
  + Presentation Layer
  + Service Layer
    - Integration Services
    - Business Services
    - Common Services
    - Technical Services
    - Security Services
  + Information Layer
    - Data Services
      * Object to Relational Mapping framework
    - Transactional Data Model
    - Non-structured and Document Storage
    - Reporting
  + Integration Layer
    - Integration Design Patterns
    - Service Bus Framework
    - EMS to SOS VoteCal Message Transformations
    - SOS VoteCal Replies
      * SOS VoteCal Payload to EMS Message Transformation
      * Reply Message Processing
      * Error Processing
        + Logging

### Deliverable 4: Final Performance Test Plan

It is expected that at this phase the Performance Test Plan is updated to reflect any modifications or updates that were introduced during the UAT phase.

The performance test plan is expected to describe the testing that will be completed to ensure that the EMS will function uninterrupted and efficiently under periods of high usage (typically coinciding with a California election). The types of performance testing that should be addressed are as follows:

* Load testing – A test of multiple users or test process emulating peak demands.
* Stress testing – Going beyond system limitations to identify actual limitations.
* Endurance testing – Test a high volume for an extended period of time.
* Resilience testing – Test loss of connectivity and service disruption.
* Recovery testing – Test how the system recovers following crashes and/or HW failures.

The Performance test plan should also include a listing of all the performance requirements, listed below and/or agreed to between the SOS and the EMS vendor, along with the testing results showing all performance requirements are met.

### Deliverable 7: Final EMS Code delivery

The SOS expects that the EMS vendor submit the latest version of the EMS code, representing the EMS code base that will be used in Production. The SOS will review the code using the process outlined in section 3.2.7.

This version of the code is the version expected to be installed in the county and will be required to be placed in an SOS specified escrow account between the pilot county and the EMS vendor. Each county running the EMS will be a beneficiary of the master escrow agreement.

### Deliverable 9: User Acceptance Test Plan

A User Acceptance Test (UAT) plan will be developed by the EMS vendor in collaboration with pilot counties, and the SOS at the start of the UAT phase.  Executing the plan will ensure that the County and SOS are able to migrate data to the new EMS, successfully register voters, do list maintenance and run an election using the EMS.

* Data Migration tests and test results will be written by the county and EMS vendor.
  + It is expected that at the beginning of UAT execution the EMS vendor and the county have already rehearsed the data migration tasks and verified that all production data for the county can be migrated successfully.
* County specific test cases will be written and executed by the County and the EMS vendor.
* VoteCal integration test cases will be written and executed by the County, SOS and the EMS vendor.

All test cases will be drafted in excel using a UAT test script template that the SOS will provide. Each test step will include detailed instructions for executing the step with expected results, the party responsible for executing the step (County or SOS) as well as specific timeframes for completing test steps such that County and SOS steps are grouped together to the degree possible.  The EMS vendor will be responsible for identifying data to be used for each test case and will populate the UAT test scripts with the data to be used.

The County, EMS vendor and the SOS will review all test scripts (walkthrough sessions will be conducted as needed) and the SOS will post the reviewed test scripts to a repository where they can be tracked and updated by all during execution.

## Final Certification

The EMS vendor must gain county support for final acceptance of SOS certification. To that end the EMS Vendor must submit to the pilot county for review, and the pilot county must approve, the following county specific deliverables:

* System User Manual
* System Training Plan
* County Migration Plan

The EMS vendor must also show signed intent of county to move to the vendor’s EMS.

### Application for Initial Certification

Then the EMS vendor must complete the EMS Certification Application as an “Initial Certification” with a “Final Submission” of the System Documentation Package (SDP) with signature and the SOS must sign as well for the EMS to become fully certified. This Final submission must be submitted along with all latest versions of SOS and county deliverables included as described below:

#### SOS approved Software System Design Document

This is the Software System Design Document that was submitted and approved in the UAT phase. This document describes the logical design of the software. This documentation should clearly indicate the various modules of the software, their functions, and their interrelationships with each other. This includes the database design, input formats, output layouts, human machine interfaces, and external interfaces. Design document sections should be mapped to and cover all requirements.

#### SOS approved System Architecture Document

This is the System Architecture Document that was submitted and approved in the UAT phase and it describes the logical representation of the system, consisting of system components, systems developed, communication paths and end points, that work together to implement the overall system in the state of California.

#### SOS approved EMS Software Code

This is the EMS Software Code that was submitted and approved in the UAT phase. EMS Software Code must represent the version being submitted for certification, including all county installation and setup instructions/requirements.

#### SOS approved System Test Plan and results

This is the System Test Plan that was submitted and approved in the System Testing phase. The System Test Plan includes test scripts with detailed instructions, including actions and expected results, describing steps to carry out all remediated EMS functionality. Test results shall be provided including pass fail percentages for test executed, descriptions of all deficiencies identified and/or resolved, and confirmation of successful completion of the given test effort.

#### SOS approved Performance Test Plan and results

This is the Performance Test Plan that was submitted and approved in the UAT phase. The Performance Test Plan includes descriptions of all the performance (or load/volume) related testing that has been conducted on the remediated EMS to verify that performance requirements have been met. Results will include pass fail percentages, descriptions of all deficiencies identified and/or resolved, and confirmation of successful completion of the given test effort.

#### SOS approved Security Test Plan and results

This is the Security Test Plan that was submitted and approved in the System Testing phase. The Security Test Plan shall include descriptions of all the security related testing that has been conducted, including full source code review and penetration testing, on the remediated EMS to verify that security requirements and drafted security regulations have been met. Results shall include pass fail percentages, descriptions of all deficiencies identified and/or resolved, and confirmation of successful completion of the given test effort.

#### Pilot county approved System User Manual

This is documentation that must be submitted to, and approved by, the county and shall include “how to” instructions for all EMS functionalities supplied to the customer for use by the person(s) who will use the system. Documentation shall cover all requirements of the system, including all interactions with the VoteCal system. User documentation should be developed to accompany current and existing VoteCal guidance documentation such as; Confidential Voters, Conditional Voter Registration, EMS Messages, Official List, Registration Date, DMV Change of Address, Synch Check, Voter Information Guide, Report of Registration, Public Voter Data Request (PVRDR), Jury Wheel, Ballot Processing, Push Voter, and California New Motor Voter.

The SOS expects that the EMS vendor submit their full system user manual to the SOS for review by the SOS and pilot county. It is expected that the user manual audience is the county end users, and the goal of the documentation is to show county end users how to perform all functions available within the EMS including utilizing VoteCal integrations services. The documentation should be well organized, easily searchable, and include descriptive titles and subtitles. The documentation should use annotated screenshots as well as examples with end results. Finally, the EMS vendor shall provide and record a walk-though of the user manual for later viewing.

#### Pilot county approved System Training Plan

This is documentation that must be submitted to, and approved by, the county and shall include detail regarding how the EMS vendor will train county elections officials’ staff in the use of the remediated EMS, including all technical and user-facing EMS functionality. The Training Plan shall include detail on the different approaches proposed for each county that uses the vendor intends to train. For example, a large county may require a train-the-trainer approach in addition to typical training, to facilitate training to a large number of county users.

#### Pilot county approved County Migration Plan

This is documentation that must be submitted to, and approved by, the county and shall include the detailed steps to be taken to migrate an existing county from one EMS to the remediated EMS being certified and shall include roles and responsibilities for all necessary cutover activities. The County Migration Plan shall include county preparation activities required for migration readiness, contingency and fallback plans should the transition fail, and the general approach for county support through and following the cutover processes.

# EMS Deliverable review process

## Definition of Deliverable Expectations:

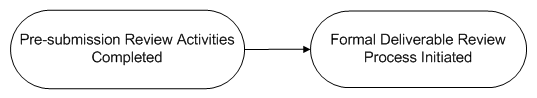
The SOS will document deliverable expectations within this EMS Certification Plan. This will establish consistency between various EMS vendors, minimize the time needed to accomplish review and obtain approval of deliverables. Deliverable expectations are expected to evolve throughout the course of review with individual EMS vendors and will be incorporated into subsequent versions of this plan to be leveraged for other EMS vendors. Individual deliverable expectations are described in section 3 - *Certification Process* and generally include, but are not necessarily limited to specific requirements, objectives, standards, general deliverable attributes, deliverable organization, and other criteria.

## Pre-submission Review Activities

Deliverables will be developed by EMS vendors and will be agreed to in concept through in collaboration with SOS staff during various deliverable development stages and prior to formal submission of the final deliverable. EMS vendors and SOS will collaborate to determine the best methods and procedures to facilitate for pre-submittal collaboration and review but typically they will involve one review of the deliverable to identify feedback and a pre-submission walkthrough, if needed, to provide feedback to the vendor.

The EMS vendor will complete these activities in order to confirm assumptions, resolve questions and better assure that emerging deliverables align with deliverable expectations. EMS vendors will be responsible for recording and addressing feedback provided. EMS vendors are expected to ensure that all deliverable-related questions and issues are resolved to the extent possible during the pre-submission deliverable activities and prior to formal Deliverable submission. Once final deliverables are formally submitted for SOS acceptance, they are expected to be error-free and contain no deficiencies.

The diagram below shows that pre-submission review activities precede the Formal Deliverable Review Process:



The following link is a template email that can be used to send a pre-review assignment to a deliverable reviewer:

[\\Sosfps4\sos\_share\Projects\HAVA\SWDb\VoteCal\EMS Certification\Deliverables\Planning Docs](file://Sosfps4/sos_share/Projects/HAVA/SWDb/VoteCal/EMS%20Certification/Deliverables/Planning%20Docs)

Note: *This link will only work if you are on the SOS network and have permissions.*

Filename: “Deliverable Review Assignment Template.docx”

## Formal Deliverable Review

EMS vendors are expected to identify modified portions of a deliverable since the pre-submission review activities to facilitate for an efficient formal review process. Each DR reviews and evaluates the deliverable to verify that:

* The deliverable conforms to and operates in accordance with all SOS expectations.
* The deliverable is comprehensive and consistent in level of detail and quality.
* The deliverable is organized in a structured manner and is consistent with the expectations set for the deliverable.

The deliverable expectations, along with the deliverable descriptions provided below are used to evaluate the deliverable to specifically determine if the deliverable is accurate, complete and can be approved.

A CTS workbook will be created by the ECM to be used by each DR to record identified deliverable deficiencies, gaps, or potential risks or issues.

Below are the CTS fields Deliverable reviewers will populate in-order to complete feedback. The Template CTS document is located at:

| Reviewer populated CTS fields | |
| --- | --- |
| Field | Definition |
| Document Version | The version of the deliverable being reviewed. |
| Deliverable Deficiency Severity Level | Deliverable Deficiency Severity Levels will be a numerical rating used to specify the impact or significance of each identified deliverable deficiency, entered into the CTS, based on the acceptance criterion that the deliverable fails to meet. Deliverable Deficiency Severity Levels will only be assigned to comments reporting deliverable deficiencies. Deliverable reviewers will record “N/A” in this column for any comments reporting a question. |
| Page | The page number (or appropriate reference number if no page numbers exist) of the Deliverable to which the comment applies. |
| Section | The section number (or location if no section numbers exist) in which the comment was made. |
| Deliverable Reviewer | The Deliverable Reviewer who identified the comment and/or who is responsible for verifying that the comment has been satisfactorily addressed in future submissions of the deliverable. |
| Comment Date | The date in which the comment was recorded in the CTS. |
| Comment | A description of the deliverable deficiency or question identified. |
| Reference Material | Optional field: If there exist any documents supporting the comment entered, a link to those documents should be included within this field. |
| Satisfactorily Addressed? | This field will only be used for corrected, resubmitted deliverables and will be completed in the updated version of the consolidated CTS that the contractor has returned explaining how each of the comments have been addressed in the corrected, resubmitted deliverable. DRs will enter a ‘yes’ or ‘no’ value in this field to indicate if a previously reported comment has been satisfactorily addressed. |

*Note: Grey columns will be populated for Deliverable Reviewer comments entered during previous review cycles for which the EMS vendor has addressed.*

DRs will attempt to identify and document any and all reasonably discoverable deficiencies including deviations between the deliverable and SOS business or technical policy as well as potential project risks or issues which could negatively impact SOS, VoteCal, California elections, or county election offices.

If a DR identifies a critical deliverable deficiency, they will immediately notify the ECM, and the VoteCal director. DRs will let the ECM know as soon as possible if they believe they will be late in providing their review of the deliverable.

Upon a corrected version of a previously submitted deliverable getting re-submitted (expected to occur only at most once per deliverable), in which SOS had previously provided the EMS vendor with a consolidated CTS, the EMS vendor will populate the below fields for each feedback provided on the CTS.

| Contractor Populated CTS fields | |
| --- | --- |
| Field | Definition |
| Resolution | A narrative description of the action that was taken to resolve the comment. If the EMS vendor addresses the comment exactly as requested in the original DRs’ comment, this field shall read “addressed as requested.” Otherwise, this field should specify how the comment has been addressed. |
| Addressed in Section | The section number (or location if no section numbers exist) in which the comment was addressed. |
| Notes | Additional information including, for example, an explanation for any comments that have been left open at re-submittal to SOS. |
| Resolved Version | The version number of the deliverable in which the comment has been resolved. |

DRs must then confirm that comments reported have been resolved by the EMS vendor and have been addressed completely and satisfactorily. DRs will be responsible for populating the ‘Satisfactorily Addressed?’ field for each addressed comment that they had previously submitted (or that have otherwise been assigned to them by the Functional Project Manager) as indicated in the ‘Deliverable Reviewer’ column of the consolidated CTS.

### Formal Deliverable Review assignment email template

The below is a template for a Formal Deliverable review assignment that will be sent out to all deliverable reviewers to initiate the formal review process.

The below link is to the formal assignment email template:

[\\Sosfps4\sos\_share\Projects\HAVA\SWDb\VoteCal\EMS Certification\Deliverables\Planning Docs](file://Sosfps4/sos_share/Projects/HAVA/SWDb/VoteCal/EMS%20Certification/Deliverables/Planning%20Docs)

Note: *This link will only work if you are on the SOS network and have permissions.*

Filename: “Deliverable Review Assignment Template.docx”

Included for convenience is sample assignment email text:

|  |
| --- |
| Hi Folks,  Attached is the [Deliverable] for formal SOS review from [EMS Vendor].  As a deliverable reviewer for this deliverable, please review and provide your feedback by [Due Date].  *Note: [Specific notes about when the Deliverable will be resubmitted]*  Record your feedback within the Comment Tracking sheet (CTS) at the below link by populating the following fields for each comment you have.   * Deliverable Reviewer * Document Version * Deliverable Deficiency Severity Level * Page/Tab or Section * Comment Date * Comment   If you had feedback or not, please send an email to VoteCalEMSCertification@sos.ca.gov by [Due Date] to indicate that your review is completed.  The below link will take you to a folder with the following files:   1. Comment tracking sheet where you’ll add your feedback. 2. EMS vendors expectations documentation. 3. SOS’s drafted expectations for the Deliverable. 4. The Deliverable to be reviewed.   Link to deliverable folder:  If you have any questions, please reach out to VoteCalEMSCertification@sos.ca.gov.  Thank you,  Sean Malone |

# Ongoing Certification

Ongoing certification includes 2 main components:

* + Annual Re-Certification process
  + SOS maintenance contract agreement

## Re-Certification Process

The recertification process is outlined within current regulations section 19067 Certified EMS. In summary EMS vendors are required to sumit versions of their EMS code to escrow at each major release and are required to provide a signed letter indicating their compliance with VoteCal annually. Belaow are the details:

1. The certified EMS vendor shall certify in writing to the Secretary of State, annually by February 1, compliance with the requirements set forth in this section, for the previous year. The EMS certification shall be in substantially the following form:  I/we hereby certify for the period commencing January 1, 20\_\_ and ending December 31, 20\_\_, that [Company] have/has done the following:
2. Adhered to the Integration Specifications;
3. Adhered to the Data Standards;
4. Implemented all applicable approved change requests;
5. Complied with all applicable federal and state laws; and
6. Deposited the current version of the EMS source code with an approved escrow facility in accordance with Section 2501 of the Elections Code and Chapter 6 of Division 7 of Title 2 of the California Code of Regulations.
7. The certified EMS vendor shall support county synchronization checks initiated by the county and/or the Secretary of State, at a minimum, monthly and no more than 30 days prior to:
   1. A Report of Registration.
   2. An Official list extract for an election.
   3. Voter Information Guide processing.
8. The certified EMS vendor shall work with county elections officials to resolve data discrepancies identified until acceptable tolerance levels for synchronization, as set forth in Section 19083, are attained by the county.
9. Defects or bugs with the certified EMS that affect the statewide voter registration system or any other certified EMS currently in use shall be logged immediately with the Secretary of State Elections Division Help Desk. Once reported to the Secretary of State Elections Division Help Desk, the defect or bug shall be categorized by the Secretary of State and resolved as follows:
   1. Critical:
      1. A critical defect or bug:
         1. prevents the accomplishment of an essential function; or
         2. jeopardizes safety, security, or causes unrecoverable data loss.
      2. For critical defects or bugs, the EMS vendor must conduct analysis and provide next steps, or provide a resolution, within one (1) business day following notification of the problem. A solution or workaround must be provided within two (2) business days of notification when possible, or by a mutually-agreed-upon date between the EMS vendor and Secretary of State.
   2. High:
      1. A high defect or bug:
         1. adversely affects the accomplishment of an essential function and there is no known workaround solution;
         2. causes recoverable data loss but with high impact to users; or
         3. impacts the reliability of public-facing functionality or data.
      2. For high defects or bugs, the EMS vendor must conduct analysis and provide next steps, or provide a resolution, within three (3) business days following notification of the problem. A solution or workaround must be provided by a mutually-agreed-upon date between the EMS vendor and Secretary of State.
   3. Medium:
      1. A medium defect or bug:
         1. affects the accomplishment of an essential function(s) and a workaround solution is known; or
         2. causes recoverable data loss.
      2. For medium defects or bugs, the EMS vendor must conduct analysis and provide next steps, or provide a resolution within 10 business days following notification of the problem. A solution or workaround must be provided by a mutually agreed upon date between the EMS vendor and Secretary of State.
   4. Low:
      1. A low defect or bug:
         1. results in user/operator inconvenience, but does not affect a required operation or mission essential function; or
         2. results in a cosmetic or documentation issue to non-public facing functionality.
      2. For low defects or bugs, the EMS vendor must conduct analysis and provide next steps, or provide a resolution within 10 business days following notification of the problem. A solution or workaround must be provided by a mutually agreed upon date between the EMS vendor and Secretary of State.

## SOS Maintenance Contract agreement

Certified EMSs shall be in contract with the SOS for maintenance and operations including implementation of change requests initiated from the SOS. Terms will be determined through mutual agreement between the SOS and the EMS vendor.

# Appendix

## Acronyms

CGI – VoteCal Systems Integration Contractor

CL – Core Lead

CTE - County Test Environment

DR – Deliverable Reviewer

ECM – EMS Certification Manager

ECP – EMS Certification Plan

EMS – Election Management System

ITD - Information Technology Division (ITD)

PMO - Project Management Office

SDP - System Documentation Package

SME – Subject Matter Expert

SOS – Secretary of State

## EMS Certification Steps by Phase

|  |  |  |
| --- | --- | --- |
| **EMS Certification Phase** | **#** | **Step to complete** |
| Initiation | 1 | Review VoteCal Materials and Certification Process |
| 2 | Complete EMS Certification Application |
| Planning | 3 | Deliverable 1: Work Breakdown Structure |
| 4 | Deliverable 2: Interim Software System Design Document |
| 5 | Deliverable 3: System Architecture Document |
| 6 | Deliverable 4: Performance Test Plan |
| 7 | Deliverable 5: Security Test Plan |
| 8 | Deliverable 6: System Test Plan |
| 9 | Deliverable 7: Interim EMS Code Delivery Expectations |
| Internal Development Testing | 10 | Deliverable 2: Software System Design Document |
| 11 | Deliverable 3: System Architecture Document |
| 12 | Deliverable 5: Security Test Plan |
| 13 | Deliverable 6: System Test Plan |
| 14 | Deliverable 7: Interim EMS Code delivery |
| System Testing | 15 | Execute System Testing |
| 16 | Deliverable 2: Interim Software System Design Document |
| 17 | Deliverable 8: System, Performance, and Security Testing Results |
| 18 | Deliverable 7: Interim EMS Code delivery |
| User Acceptance Testing | 19 | Execute UAT |
| 20 | Deliverable 2: Final Software System Design Document |
| 21 | Deliverable 3: Final System Architecture Document |
| 22 | Deliverable 4: Final Performance Test Plan |
| 23 | Deliverable 7: Final EMS Code delivery |
| 24 | Deliverable 9: User Acceptance Test Plan |
| Final Certification | 25 | Application for Initial Certification |
| 26 | SOS approved Software System Design Document |
| 27 | SOS approved System Architecture Document |
| 28 | SOS approved EMS Software Code |
| 29 | SOS approved System Test Plan and results |
| 30 | SOS approved Performance Test Plan and results |
| 31 | SOS approved Security Test Plan and results |
| 32 | Pilot county approved System User Manual |
| 33 | Pilot county approved System Training Plan |
| 34 | Pilot county approved County Migration Plan |

1. “Essential function” is defined as critical functionality at the time when it is needed for execution. [↑](#footnote-ref-2)
2. [1] “Essential function” is defined as critical functionality at the time when it is needed for execution. [↑](#footnote-ref-3)