Stage 2 Alternatives Analysis

California Department of Technology, SIMM 19B.2 (Ver. 3.0.8, 02/28/2022)

2.1 General Information

1. **Agency or State Entity Name:** Choose an item.

   If Agency/State entity is not in the list, enter here with the organization code.

   2667 – Office of the Inspector General, High-Speed Rail

2. **Proposal Name:** OIG-HSR Whistleblower Complaint Receipt and Investigation System

3. **Department of Technology Project Number (0000-000):** 2667-002

4. **S2AA Version Number:** Version 1

5. **CDT Billing Case Number:** RZX

6. Don't have a Case Number? Click here to get one.

2.2 Submittal Information

1. **Contact Information**

   Contact Name: Deputy Inspector General – Amanda Millen

   Contact Email: Amanda.Millen@oig.hsr.ca.gov

   Contact Phone: (916) 908-0922

2. **Submission Type: New Submission**

   If Withdraw, select Reason: Choose an item.

   If Other, specify reason here: Click or tap here to enter text.

   Sections Changed if an update or resubmission: (List all the sections that changed.)

   Click or tap here to enter text.

Summary of Changes: (Summarize updates made.)

Click or tap here to enter text.

3. **Attach Project Approval Executive Transmittal to your email submission.**

4. **Attach Procurement Assessment Form to your email submission.**

5. **Conditions from Stage 1 Approval** (Enter any conditions from the Stage 1 Business Analysis approval letter issued by CDT or your AIO):

   Click or tap here to enter text.

2.3 Baseline Processes and Systems

1. **Current Business Environment (Describe the current business environment of which the effort will be understood and assessed in 500 words)**

   The Office of the Inspector General, California High-Speed Rail (OIG-HSR) is a newly established, independent oversight entity tasked with investigating allegations of fraud, waste, abuse, mismanagement, and threats to public health and safety associated with California's high-speed rail project. The department began formal operations in late 2023 and is currently in the process of building out its organizational capacity, including the development of its Investigations Division.

   Currently, OIG-HSR receives whistleblower complaints exclusively through two channels: a High-Speed Rail Authority (Authority)-issued email address and a telephone hotline, both maintained by the Authority. All case-related documentation is stored within shared network drives managed by the Authority's Information Technology office. As such, the Authority—despite being the likely subject of complaints—has administrative access to communication records and stored documentation related to whistleblower complaints and investigations. This arrangement conflicts with the requirements established under Public Utilities Code §§187030 and 187032(a)(3), which prohibit the disclosure of a whistleblower's identity and call for independent oversight of the Authority's activities.

   The current process also lacks standardized workflows and investigative tracking tools. Investigations are logged manually using spreadsheets, without automated case numbering, performance metrics, audit trails, or secure digital evidence handling. This manual approach increases the risk of inconsistent documentation, unintentional data exposure, and inefficiencies in processing and oversight. Moreover, the lack of confidential digital intake or messaging capabilities reduces the likelihood that whistleblowers will feel safe coming forward, particularly those who may have sensitive information implicating Authority staff or contractors.

   Although the Authority's provision of IT services has allowed OIG-HSR to ramp up operations rapidly and cost-effectively, it simultaneously constrains the office's ability to fully meet its statutory responsibilities, follow professional investigative standards, or safeguard sensitive information. Without an independent, access-controlled whistleblower case management

system, OIG-HSR will continue to operate with critical gaps in compliance, operational security, and efficiency.

Tip: Current Environment costs will be asked for in the Financial Analysis Worksheet to be completed in Section 2.12.

Attach relevant documentation to email submission (i.e., business process, workflow, problem analysis, user/stakeholder list, research findings). If these types of documents are not available, please indicate "Not Available," and explain the reason below:

Not available reason: Click or tap here to enter text.

2. **Technical Context (Describe the technical environment of which the effort will be understood and assessed in 500 words)**

The current technical environment used by OIG-HSR is entirely reliant on IT systems provided and administered by the Authority. This includes all hardware (e.g., laptops, phones), software (e.g., Microsoft Office Suite), communication tools (email and telephone systems), and document storage (shared network drives). OIG-HSR staff access these resources through user accounts and network domains fully controlled by the Authority's Information Technology office.

No dedicated case management system is currently in place. Whistleblower complaints are received via standard email or phone calls and are manually tracked using Excel spreadsheets. Documents submitted by complainants or developed during investigations are stored in folder-based directories without case-specific access restrictions, audit trails, version control, or role-based permissions. Any Authority IT administrator with appropriate credentials could access these files, making true data segregation impossible.

There are no technical safeguards such as encryption at rest for sensitive case files, identity authentication beyond basic user credentials, or logging of document access or edits. Similarly, OIG-HSR cannot currently conduct secure digital communication with whistleblowers, as all communications pass through Authority-managed systems. In addition to the challenges with lacking a secure method to collect the initial compliant, there is also no secure venue for two-way communication between the OIG-HSR and the submitter following the submission of the complaint.

Because OIG-HSR does not have its own network or IT support structure, it cannot isolate investigative workflows or guarantee whistleblower confidentiality under the existing technical setup. Furthermore, the absence of a platform that enforces professional standards for chain of custody, supervisory review, or digital evidence handling limits the ability of investigators to maintain reliable documentation of case activity.

The technical gap is not due to a lack of expertise or desire within OIG-HSR but rather due to the structural limitations of relying on the very entity it oversees for IT services. A separate, FedRAMP-compliant SaaS platform is needed to provide a secure environment for case intake, processing, and documentation while maintaining integration with existing end-user hardware.

Attach relevant documentation to email submission (i.e., logical system environment diagrams, system interactions, business rules, application flows, stakeholder information, data flow charts). If these types of documents are not available, please indicate “Not Available,” and explain the reason below:

Not available reason: N/A

3. **Data Management (Enter the information to indicate the data owner and custodian of the current system, if applicable.)**

   Data Owner Name: HSR-OIG

   Data Owner Title: Deputy Inspector General

   Data Owner Business Program area: Whistleblower Complaints

   Data Custodian Name: HSR-OIG

   Data Custodian Title: Deputy Inspector General

   Data Custodian Technical area: N/A

   Security - Data Classification and Categorization No

   Security - Privacy Threshold & Impact Assessment. No

4. **Existing Data Governance and Data**

   a) Do you have existing data that must be migrated to your new solution?

      Answer (Unknown, Yes, No): No

      If data migration is required, please rate the quality of the data.

         Select data quality rating: Choose an item.

   b) Does the Agency/state entity have an established data governance body with well-defined roles and responsibilities to support data governance activities?

      Answer (Unknown, Yes, No): No

      If Yes, include the data governance organization chart as an attachment to your email submission.

   c) Does the Agency/state entity have data governance policies (data policies, data standards, etc.) formally defined, documented, and implemented?

      Answer (Unknown, Yes, No): Yes

      If Yes, include the data governance policies as an attachment to your email submission.

   d) Does the Agency/state entity have data security policies, standards, controls, and procedures formally defined, documented, and implemented?

      Answer (Unknown, Yes, No): Yes

If Yes, attach the existing documented security policies, standards, and controls used to your email submission.

e) Does the Agency/state entity have user accessibility policies, standards, controls, and procedures formally defined, documented, and implemented?

Answer (Unknown, Yes, No): Yes

If Yes, attach the existing documented policies, accessibility governance plan, and standards used to the email submission.

5. **Security Categorization Impact Table**

Consult the SIMM 5305-A Information Security Program Management Standard - Security Categorization Impact Table.

Attach a table (in PDF) that categorizes and classifies the agency/state entity's information assets related to this effort (e.g., paper and electronic records, automated files, databases requiring appropriate protection from unauthorized use, access, disclosure, modification, loss, or deletion). Each information asset for which the agency/state entity has ownership responsibility shall be inventoried and identified.

6. **Security Categorization Impact Table Summary**

Consult the SIMM 5305-A Information Security Program Management Standard - Security Categorization Impact Table to provide potential impact levels of the following areas:

Confidentiality: High

Integrity: Medium

Availability: Low

7. **Technical Complexity Score: 0.9**

(Attach a SIMM Section 45 Appendix C with Business and Technical Complexity sections completed to the email submission.)

2.4 Requirements and Outcomes

At this time in the project planning process, requirements and outcomes should be documented and indicative of how the Agency/State Entity envisions the final solution. This shall be accomplished either in the form of mid-level requirements (predictive methodology)/business capabilities or representative epics and user stories (adaptive methodology) that will become part of the product backlog. The requirements or representative epics and user stories must tie back to the Objectives detailed in the Stage 1 Business Analysis. Regardless of which tool/method is used, an understanding of the following, at a minimum, must be clearly articulated:

- Functional requirements
- Expected user experience(s)
- Expected system outcome

- Expected business operations (e.g., How do you envision operations in the future?)
- Alignment to the project's objectives identified in Stage 1
- Product ownership (e.g., Who owns these requirements?); and
- Verification of need(s) fulfillment (e.g., How will success be measured?)

Tip: If providing requirements, the recommended range of requirements is between 50 and 100.

Attach Requirements and/or Outcomes narratives, mid-level requirements, and/or epics/user stories to submission email.

Requirements have been attached as:

2.04.0 Midlevel_Solution_Requirements.xlxm

2.5 Assumptions and Constraints

Relevant assumptions and constraints help define boundaries and opportunities to shape the scope and complexity of the project.

Assumption: OIG-HSR staff will continue to use Authority-provided IT hardware (laptops, phones) to access the new system.

> **Description/Potential Impact**: Software procured is subject to Authority-provided hardware technical specifications and security
>
> **Description/Potential Impact**: Authority-provided hardware becomes unavailable or restricted, or if auxiliary equipment needs to be procured, increasing project costs and delaying implementation. However, state law requires the Authority to provide needed IT services and equipment to the OIG-HSR and tis staff, making this impact extremely unlikely.

Assumption: Vendors under consideration must offer FedRAMP-compliant hosting environments that meet State of California information security requirements.

> **Description/Potential Impact**: OIG-HSR is only considering FedRAMP-compliant vendors

Assumption: FY 2025–26 implementation funding will be approved as part of the budget process.

> **Description/Potential Impact**: Without approved funding, project execution cannot proceed, resulting in a continued inability to comply with confidentiality laws. However, project costs for FY2025-26 are included in an approved budget change proposal from OIG-HSR that is currently included in the Legislature's approved budget,

Assumption: Authority IT will allow secure and limited system access (e.g., network routing, endpoint access) without having data-level visibility.

> **Description/Potential Impact**: As noted above, the Authority is legally required to provide network access to OIG-HSR, but any challenges in establishing this arrangement could result in delays. OIG-HSR has listed the Authority as a project stakeholder for this reason, and its management has been in communication with IT executives at the Authority to plan for implementing the eventual project on its network.

Assumption: OIG-HSR can administer the selected solution without needing to establish a full internal IT function.

> **Description/Potential Impact**: If vendor or system limitations require significant in-house technical support, it may necessitate staffing or procurement changes, increasing project complexity.

Assumption: The user base (internal and external) will require minimal training due to the vendor's intuitive design and provided support materials.

> **Description/Potential Impact**: If training needs are underestimated, it could delay rollout and decrease early adoption or accurate data entry.

Assumption: No major legislative or regulatory changes related to confidentiality or case management will occur during project implementation.

> **Description/Potential Impact**: New legislation or regulations could require rework or system changes, impacting cost and timeline.

Assumption: The SaaS will be supplemented by a small amount of additional equipment and software, including one off-network scanner and laptop, and a VoIP tool to facilitate collection and confidential processing of hard-copy complaints and evidence as well as confidential phone calls and meetings with whistleblowers and witnesses.

> **Description/Potential Impact**: Some additional hardware may need to be procured, as well as an additional communication software tool such as Zoom

Constraint: The system must be hosted separately from Authority infrastructure.

> **Description/Potential Impact**: Hosting the system on Authority-controlled servers would violate confidentiality and independence requirements and may invalidate the project's statutory objectives.

Constraint: Authority staff must not be granted any administrative or user-level access to the system.

> **Description/Potential Impact**: Any level of access may compromise the confidentiality of whistleblower data and deter future reporting.

Constraint: The system must be fully operational before the end of FY 2025–26

> **Description/Potential Impact**: Delays may result in failure to meet strategic objectives and further delay OIG-HSR's ability to demonstrate full compliance with statutory mandates for confidentiality.

Constraint: The system must comply with confidentiality provisions in Public Utilities Code 187032(a)(3).

Description/Potential Impact: Non-compliance may expose the State to legal risk and undermine the OIG-HSR's credibility and mission.

Constraint: The selected system must support anonymous intake and secure messaging features.

Description/Potential Impact: Inability to support anonymous complaints or confidential communication would likely reduce the willingness of some to come forward with a complaint

TIP: Copy and paste to add Assumptions/Constraints with Descriptions/Impacts as needed.

2.6 Dependencies

Dependencies are elements or relationships in a project reliant on something else occurring before the function, service, interface, task, or action can begin or continue.

Dependency Element: Authority Network Access

Dependency Description: OIG-HSR requires continued ability to use Authority-provided hardware and internet to connect to the new system while ensuring that no Authority staff have access to the whistleblower case management system.

Dependency Element: FY 2025–26 Budget Approval

Dependency Description: Project planning is contingent on funding approval through the FY 2025–26 Budget Change Proposal submitted in August 2024. Project execution will be contingent on approval of project funding to be requested in a FY 2026-27 Budget Change Proposal

Dependency Element: Vendor FedRAMP Certification

Dependency Description: The selected vendor must maintain active FedRAMP certification for hosting whistleblower data in compliance with federal and state security requirements.

Dependency Element: Timely Procurement Execution

Dependency Description: Project relies on successful completion of competitive procurement activities and contract execution before the end of fiscal year 2025-2026

Dependency Element: Security & Privacy Compliance Reviews

Dependency Description: Approval of a Privacy Threshold Assessment (PTA), as well as compliance with state security policies and applicable IT policies, is required for go-live.

Dependency Element: Authority User Adoption

Dependency Description: Whistleblower users, including Authority staff and contractors, must begin using new web and phone submission channels after deployment. OIG-HSR must support awareness and trust-building communications to enable this transition.

TIP: Copy and paste to add Dependency Elements and Descriptions as needed.

2.7 Market Research

Market Research (CDT Market Research Guidelines) determines whether products or services available in the marketplace can meet the business needs identified in this proposal. Market Research can also determine whether commercial practices regarding customizing/modifying products or tailoring services are available, or even necessary, to meet the business needs and objectives of the business.

Before undertaking a Market Research approach. Contact your PAO Manager to schedule a collaborative review to review planning to date and discuss the procurement approach.

1. **Project Management Methodology:** Adaptive Approach (Agile)

2. **Procurement approach recommended:** Standard Procurement

3. **Market Research Approach**

   Provide a concise narrative description of the approach used to perform market research.

   To inform its procurement strategy, OIG-HSR conducted targeted market research on whistleblower case management software, evaluating three leading solutions

   1. Opexus
   2. Navex3.
   3. CaseIQ

   The research focused on each vendor's ability to meet 18 defined feature areas related to topics like confidentiality, security, case tracking, and investigative workflows. OIG-HSR's evaluation involved a structured feature comparison, supplemented by secondary research from vendor documentation and industry sources.

   After market research was concluded, Opexus emerged as the most complete and public sector aligned solution for OIG HSR, supporting all 18 features and incorporating standards for investigations. The full table and analysis can be found in supporting documentation attached to the S2AA.

4. **Market Research Artifacts**

   Market Research Artifacts can include internet research, collaboration with other governmental entities, or other documentation.

   Attach Market Research artifacts to the email submission.

2.8 Viable Alternative Solutions

The CDT expects Agencies/state entities to conduct a thorough analysis of all feasible alternatives that will meet the proposal's objectives and requirements. Agencies/state entities should provide at minimum the three (3) most viable solutions, one (1) of which could be leveraging and/or enhancing the existing solution (if applicable).

1. **Viable Alternative Solution #1**

Name: Procurement of SaaS Whistleblower Case Management System

Description: Procure and implement a FedRAMP-compliant SaaS solution from a government-focused vendor such as Opexus. This platform would support secure, confidential whistleblower complaint intake, investigation workflows, supervisory reviews, document management, and performance tracking in compliance with HSR Inspector General standards. The SaaS would be supplemented by a small amount of additional equipment, including one off-network scanner and laptop, and a VoIP tool to facilitate confidential collection and processing of hard-copy complaints and evidence as well as confidential phone calls and meetings with protected whistleblowers and witnesses.

Why is this a viable solution? Please explain:

This solution aligns directly with OIG-HSR's legal mandate to restrict access to whistleblower data, support anonymous complaints, and maintain investigative integrity. Market research found SaaS solutions that meet most or all of the stated mandatory requirements and supports the unique needs of public-sector investigative agencies. OIG-HSR's plan to acquire the small amount of additional equipment discussed above will address any requirements not fully met by SaaS solutions.

Approach

Increase staff – new or existing capabilities: No

Modify the existing business process or create a new business process: No

Reduce the services or level of services provided: No

Utilize new or increased contracted services: Yes

Enhance the existing IT system: No

Modify Statute/Policy/Regulations: No

Please Specify: Click or tap here to enter text.

Create a new IT system: No

Other: No Specify: Click or tap here to enter text.

Architecture Information

Business Function(s)/Process(es): Whistleblower Complaint Process

TIP: Copy and paste or click the + button in the lower right corner to add business processes with the same application, system, or component; COTS/Cloud Technology or custom solution; runtime environment; system interfaces, data center location; and security.

Conceptual Architecture

Attach a copy of the conceptual architecture to your email submission.

COTS/SaaS/Cloud Technology or Custom: COTS/SaaS/Cloud Technology

Name/Primary Technology: Opexus

TIP: Copy and paste or click the + button in the lower right corner to add system software information if the application, system, or component uses additional system software.

Explain Existing System Interfaces: N/A

Explain New System Interfaces: N/A

Data Center Location of the To-be Solution: Agency/state entity operated by agency/state entity

If Other, specify: Click or tap here to enter text.

Security

Access

Public: Yes

Internal State Staff: Yes

External State Staff: No

Other: No Specify: Click or tap here to enter text.

Type of Information (Select Yes or No for each to identify the type of information that requires protection. See the SAM Section 5305.5 for more information.)

Personal: Yes

Health: No

Tax: No

Financial: No

Legal: Yes

Confidential: Yes

Other: No Specify: Click or tap here to enter text.

Protective Measures (Select Yes or No to identify the protective measures used to protect information.)

Technical Security: Yes

Physical Security: Yes

Backup and Recovery: Yes

Identity Authorization and Authentication: Yes

Other, specify: Click or tap here to enter text.

Total Viable Alternative #1 Solution Cost (copy from FAW – Executive Cost Summary tab, cells E7 through E11):

Planning Costs: $534,294

One-Time (Project) Costs: $480,163

Total Future Ops. IT Staff OE&E Costs: $246,400

Total Proposed Cost: $1,260,857

Annual Future Ops. Costs (M&O): $115,700

2. **Viable Alternative Solution #2**

Name: Custom Development of a Whistleblower System

Description: Develop a fully customized whistleblower case intake and management system using state-contracted software developers or vendors. The system would be built to meet OIG-HSR's specific statutory and operational needs, including secure intake, anonymous messaging, investigation workflows, and compliance tracking.

Why is this a viable solution? Please explain:

Custom development could produce a system tailored exactly to OIG-HSR's needs and policy environment. This approach would offer long-term flexibility and control over workflows, data storage, and reporting. However, it would require more resources, time, and security validation.

Approach

Increase staff – new or existing capabilities: No

Modify the existing business process or create a new business process: Yes

Reduce the services or level of services provided: No

Utilize new or increased contracted services: Yes

Enhance the existing IT system: No

Modify Statute/Policy/Regulations: No

Please Specify: Click or tap here to enter text.

Create a new IT system: Yes

Other: No Specify: Click or tap here to enter text.

Architecture Information

Business Function(s)/Process(es): Whistleblower Complaint Process

TIP: Copy and paste or click the + button in the lower right corner to add business processes with the same application, system, or component; COTS/Cloud Technology or custom solution; runtime environment; system interfaces, data center location; and security.

Conceptual Architecture

Attach a copy of the conceptual architecture to your email submission.

COTS/SaaS/Cloud Technology or Custom: Custom

Name/Primary Technology: Custom Development

TIP: Copy and paste or click the + button in the lower right corner to add system software information if the application, system, or component uses additional system software.

Explain Existing System Interfaces: N/A

Explain New System Interfaces: N/A

Data Center Location of the To-be Solution: Agency/state entity operated by agency/state entity

If Other, specify: Click or tap here to enter text.

Security

Access:

Public: Yes

Internal State Staff: Yes

External State Staff: No

Other: No Specify: Click or tap here to enter text.

Type of Information (Select Yes or No for each to identify the type of information that requires protection. See the SAM Section 5305.5 for more information.)

Personal: Yes

Health: No

Tax: No

Financial: No

Legal: Yes

Confidential: Yes

Other: No Specify: Click or tap here to enter text.

Protective Measures (Select Yes or No to identify the protective measures used to protect information.)

Technical Security: Yes

Physical Security: Yes

Backup and Recovery: Yes

Identity Authorization and Authentication: Yes

Other, specify: Click or tap here to enter text.

Total Viable Alternative #2 Solution Cost (copy from FAW – Summary tab, cell AL33):

Total Proposed Cost: $4,079,165

3. **Viable Alternative Solution #3**

Name: Maintain Current Intake Process via Email and Hotline

Description: Continue using the Authority-provided phone and email systems to receive whistleblower complaints. Investigations would be logged manually using spreadsheets and Authority-hosted file systems.

Why is this a viable solution? Please explain:

This is the lowest-cost option requiring no system changes or procurement. However, it fails to meet statutory confidentiality requirements and professional standards, and introduces significant risk by allowing Authority IT access to sensitive data.

Approach

Increase staff – new or existing capabilities: No

Modify the existing business process or create a new business process: No

Reduce the services or level of services provided: Choose Yes or No.

Utilize new or increased contracted services: Yes

Enhance the existing IT system: No

Modify Statute/Policy/Regulations: No

Please Specify: Click or tap here to enter text.

Create a new IT system: No

Other: Choose Yes or No. Specify: Click or tap here to enter text.

Architecture Information

Business Function(s)/Process(es): Whistleblower Complaint Process

TIP: Copy and paste or click the + button in the lower right corner to add business processes with the same application, system, or component; COTS/Cloud Technology or custom solution; runtime environment; system interfaces, data center location; and security.

Conceptual Architecture

Attach a copy of the conceptual architecture to your email submission.

COTS/SaaS/Cloud Technology or Custom: Custom

Name/Primary Technology: Email and Phone

TIP: Copy and paste or click the + button in the lower right corner to add system software information if the application, system, or component uses additional system software.

Explain Existing System Interfaces: No System Interfaces

Explain New System Interfaces: No New System Interfaces

Data Center Location of the To-be Solution: Agency/state entity operated by agency/state entity

If Other, specify: Click or tap here to enter text.

Security

Access:

Public: Yes

Internal State Staff: Yes

External State Staff: No

Other: No Specify: Click or tap here to enter text.

Type of Information (Select Yes or No for each to identify the type of information that requires protection. See the SAM Section 5305.5 for more information.)

Personal: Yes

Health: No

Tax: No

Financial: No

Legal: Yes

Confidential: Yes

Other: No Specify: Click or tap here to enter text.

Protective Measures (Select Yes or No to identify the protective measures used to protect information.)

Technical Security: Yes

Physical Security: Yes

Backup and Recovery: Yes

Identity Authorization and Authentication: Yes

Other, specify: Click or tap here to enter text.

Total Viable Alternative #3 Solution Cost (copy from FAW – Summary tab, cell AL50):

Total Proposed Cost: $421,294

2.9 Project Organization

Project planning includes the process of identifying how and when specific labor skill sets are needed to ensure that the proposed project has sufficient staff with the appropriate knowledge and experience by the time the project moves into execution. All staff identified in the following sections should be included in the Financial Analysis Worksheet to be completed in Section 2.12.

1. **Project Organization Chart:**

   Attach the Project Organization Chart to your email submission.

2. **Is the department running this project as a matrixed or projectized organization?**

   Projectized

In each of the following sections, provide a concise description of the approach to staffing the proposed project including contingencies for business/program, IT, or administrative areas to maintain ongoing operations in conjunction with the proposed project.

1. **Administrative**

   Administrative functions will be supported by OIG staff. This includes logistical coordination, document management, meeting facilitation, and maintaining project documentation and records. OIG staff will ensure these functions are performed in parallel with ongoing operations to minimize disruption to core responsibilities.

2. **Business Program**

   OIG staff will serve as end users and as subject matter experts contributing business knowledge throughout the project, particularly during requirements definition, design validation, and functional testing and User Acceptance Testing. While temporary deferral of lower-priority activities may be used to manage workload during product installation, the procurement of an industry standard SaaS application should minimize the amount of support needed during implementation.

3. **Information Technology**

   General IT infrastructure support will continue to be provided by the Authority, while the vendor will be responsible for configuring, operating, and maintaining the system. Because the system is externally hosted, no additional burden is expected on internal IT staff. OIG staff will coordinate with the vendor for secure access, user provisioning, and ongoing support as needed.

4. **Testing**

   System testing responsibilities will be shared between the vendor and OIG. The vendor will conduct system integration testing and technical testing, while OIG staff will be responsible for

developing user acceptance test scripts, coordinating test sessions, and validating that the system meets business needs.

5. **Data Conversion/Migration**

   Data conversion is not applicable for this project, as the existing process is manual and no legacy case data will be migrated into the new system.

6. **Training**

   The vendor will provide video-based training and/or live virtual training sessions tailored to OIG roles. This training approach will minimize impact to OIG resources and allow for self-paced learning and adoption.

7. **Organizational Change Management**

   OCM activities related to the project will include project announcements and communications to end users. OIG will apply change management strategies throughout implementation. These include early stakeholder involvement, regular project updates, training tailored to specific roles, and active communication to ensure business readiness and promote user adoption of the new system.

8. **Resource Capacity/Skills/Knowledge for Stage 3 Solution Development**

This narrative should include the experience level and quantity of procurement, contract management, and budget staff who will be responsible for the Stage 3 Solution Development.

Stage 3 will be supported by the same OIG team that led Stage 2. This team includes experienced staff in procurement, contract oversight, and budget planning. Their direct involvement in developing the Stage 2 alternatives and conducting market research ensures continuity and preparedness as the project transitions to solution development, solicitation, and vendor selection.

2.10 Project Planning

1. **Project Management Risk Assessment**

   Updated Project Management Risk Score: 1.1

   Attach Updated PM Risk Assessment to your email submission. SIMM Section 45A

2. **Project Charter**

   Is your project charter approved by the designated Agency/state entity authority and available for the Department of Technology to review? **Choose**: 'Yes,' 'No,' or 'Not Applicable.' If 'No' or 'Not Applicable,' provide the artifact status in the space provided.

Project Charter (Approved): Yes

Status: Click or tap here to enter text.

Attach a copy of the Project Charter to your email submission.

3. **Project Plans**

Are the following project management plans or project artifacts approved by the designated Agency/state entity authority and available for the Department of Technology to review? **Choose**: 'Yes,' 'No,' or 'Not Applicable.' If 'No' or 'Not Applicable,' provide the artifact status in the space provided.

Note: For Low to medium complexity and cost projects, discuss with your PAO manager the option of submitting a Master Project Management Plan in place of individual plans.

Scope Management Plan (Approved): Yes

Status: Click or tap here to enter text.

Communication Management Plan (Approved): Yes

Status: Click or tap here to enter text.

Schedule Management Plan (Approved) : Yes

Status: Click or tap here to enter text.

Procurement Management Plan (Approved): Yes

Status: Click or tap here to enter text.

Requirements Management Plan (Approved): Yes

Status: Click or tap here to enter text.

Stakeholder Management Plan (Draft): Yes

Status: Click or tap here to enter text.

Governance Plan (Draft): Yes

Status: Click or tap here to enter text.

Contract Management Plan (Draft): Yes

Status: Click or tap here to enter text.

Resource Management Plan (Draft): Yes

Status: Click or tap here to enter text.

Change Control Management Plan (Draft): Yes

Status: Click or tap here to enter text.

Risk Management Plan (Draft + Risk Log): Yes

Status: Click or tap here to enter text.

Issue and Action Item Management Plan (Draft + Issue Log): Yes

Status: Click or tap here to enter text.

Cost Management Plan (Approved if planning BCP approved): Yes

Status: Click or tap here to enter text.

4. **Project Roadmap (High-Level)**

   Attach a high-level Project Roadmap showing remainder of planning phase and transition into execution phase to the email submission.

   a) Planning Start Date: 8/8/2024

   b) Estimated Planning End Date: 6/30/2026

   c) Estimated Project Start Date: 7/1/2026

   d) Estimated Project End Date: 6/30/2028

2.11 Data Cleansing, Conversion, and Migration

If in Section 2.3 (above) the answer to the question "Do you have existing data that must be migrated to your new solution?" was marked "Yes," please complete this section.

The California Department of Technology recommends having a Data Consultant start data cleansing, conversion, and migration activities as soon as possible.

Identify the status of each of the following data activities. If "Not Applicable" is chosen, explain why the activity is not applicable or if "Not Started" is chosen, explain when the activity will start and its anticipated duration:

1. **Current Environment Analysis: Not Applicable**

   Click or tap here to enter text.

2. **Data Migration Plan: Not Applicable**

   Click or tap here to enter text.

3. **Data Profiling: Not Applicable**

   Click or tap here to enter text.

4. **Data Cleansing and Correction: Not Applicable**

   Click or tap here to enter text.

5. **Data Quality Assessment: Not Applicable**

   Click or tap here to enter text.

6. **Data Quality Business Rules: Not Applicable**

   Click or tap here to enter text.

7. **Data Dictionaries: Not Applicable**

   Click or tap here to enter text.

8. **Data Conversion/Migration Requirements: Not Applicable**

   Click or tap here to enter text.

2.12 Financial Analysis Worksheets

Attach F.2 Financial Analysis Worksheet(s) to the email submission.

End of agency/state entity document.

Please ensure ADA compliance before submitting this document to CDT.

When ready, submit Stage 2 and all attachments in an email to ProjectOversight@state.ca.gov.

Department of Technology Use Only

Original "New Submission" Date: 7/1/2025

Form Received Date: 7/1/2025

Form Accepted Date: 7/1/2025

Form Status: In Analysis

Form Status Date: 7/1/2025

Form Disposition: Approved

Form Disposition Date: 8/26/2025