Stage 1 Business Analysis

California Department of Technology, SIMM 19A.3 (Ver. 3.0.9, 02/01/2022)

1.1 General Information

1. **Agency or State Entity Name: 4150 - Managed Health Care, Department of**

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

    Click or tap here to enter text.

2. **Proposal Name and Acronym: Identity and Access Management (IDAM)**

3. **Proposal Description: (Provide a brief description of your proposal in 500 characters or less.)**

    The DMHC proposes to add data management capabilities to support unified user identity and persona management. The DMHC seeks to implement an Enterprise Identity and Access Management (IDAM) that will enable the department to effectively and efficiently manage external user authentication and authorization using industry best practices. This Enterprise IDAM will expand the scope and availability of the current system to provide authentication and authorization with modern protocols, multi-factor authentication (MFA), single sign-on (SSO) capability, and modern accessible user interfaces. These features will lay the foundation for DMHC to modernize applications across multiple platforms and meet security mandates.

4. **Proposed Project Execution Start Date: 7/1/2026**

5. **S1BA Version Number: Version 1**

1.2 Submittal Information

1. **Contact Information**

    Contact Name: Ralph Cesena

    Contact Email: ralph.cesena@dmhc.ca.gov

    Contact Phone: +1 916-879-5792

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 this is a Submission Update: (List all sections 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** **Stage 1 Project Reportability Assessment** to your email submission.

1.3 Business Sponsorship

1. **Executive Champion (Sponsor)**

   Title: Deputy Director Office of Technology and Innovation - Chief Information Officer

   Name: Ralph Cesena

   Business Program Area: Office of Technology and Innovation

2. **Business Owner**

   Title: Chief Information Security Officer

   Name: Justin Tomek

   Business Program Area: Office of Technology and Innovation

3. **Product Owner**

   Title: Chief Information Security Officer

   Name: Justin Tomek

   Business Program Area: Office of Technology and Innovation

TIP: Copy and paste or click the + button in the lower right corner on any section to add additional Executive Champions, Business Owners, or Product Owners with their related Business Program Areas as needed.

1.4 Stakeholder Assessment

The Stakeholder Assessment is designed to give the project team an overview of communication channels that the state entity needs to manage throughout the project. More stakeholders may result in increased complexity to a project.

1. **Indicate which of the following are interested in this proposal and/or the outcome of the project. (Select 'Yes' or 'No' for each.)**

   State Entity Only: Yes

   Other Departments/State Entities: Yes

   Public: Yes

   Federal Entities: No

   Governor's Office: No

   Legislature: No

   Media: No

   Local Entities: No

   Special Interest Groups: No

   Other: No

2. **Describe how each group marked 'Yes' will be involved in the planning process.**

   The Department of Managed Health Care (DMHC) will participate in the PAL process and seek approval from CalHHS Agency and the California Department of Technology. The DMHC will manage the project, identify the requirements, procure / develop / configure the technology solution, test the solution, and implement in production. The DMHC will identify resources, including possible use of external consultants, who will be members of this project team performing these activities.

   Other entities such as the Department of Health Care Services and public users log on to applications using accounts assigned to them. Once the accounts are consolidated through this project, they will log on using the consolidated account. Such external entities will not be involved in the planning process for this project.

1.5 Business Program

1. **Business Program Name:** Office of Technology and Innovation

2. **Program Background and Context:** Provide a brief overview of the entity's business program(s) current operations.

The Office of Technology and Innovation (OTI) provides technology support to the DMHC including hardware, software, information technology project management and information security services. The Information Security Office (ISO), within the OTI, orchestrates efforts and provides services to protect the information assets that are important to the DMHC. The ISO collaborates with partners throughout the DMHC, California Health and Human Services Agency as well as the State Information Security Office to build and maintain a comprehensive cybersecurity program, which includes and is not limited to the IDAM system. The IDAM system provides capabilities to implement user authentication and authorization to ensure, monitor and manage appropriate access to all information technology systems and solutions.

The Information Security Office was established in November 2018 and has been providing information security services to the DMHC since then. These services include coordination of information security audits, responding to findings and working with information technology partners to implement information security solutions. Technology Letter (TL) 23-01 identifies the key standards to be implemented through the IDAM solution. SIMM 5360-C requires the implementation of MFA for external-facing applications. TL-2301 states that any publicly accessible information asset that stores, processes, transmits or visually presents confidential, sensitive, or personal information will be subjected to SIMM 5360-C & D. Digital Identities for information assets will be required to have an additional form of authentication based on the information assets Authenticator Assurance Level defined in SIMM 5360 C & D. This will provide an additional layer of security, which will help reduce risk of nefarious activities by internal and external threats.

The current IDAM solution , Okta, was implemented in May 2023 to further strengthen the information security around all external facing applications. These external facing applications are RBO Financial Reporting System, Vendor Price Quotation System (PTS), Health Plan Web Portal, Provider Complaint System (PCS), Joint Filing Workgroup, and Consumer Participation Program. Okta provides MFA capabilities for these external facing applications and limits access to health plan users who are authorized and authenticated for such access. External users login to these systems to submit filings to the DMHC electronically. The MFA mechanism protects sensitive and confidential data from unauthorized access. Okta requires individualized logins for each application but does not provide single sign-on capabilities.

3. **How will this proposed project impact the product or services supported by the state entity?**

The IDAM enhancement will upgrade DMHC’s application authentication and authorization technology and allows for seamless integration between legacy applications and modern cloud platforms. This is a foundational step in the Department’s application modernization initiatives aimed at leveraging modern application development platforms to efficiently deliver business solutions. The reduction in the IDAM’s technology debt increases operational and application maintenance efficiencies and enables the Department to swiftly meet application-related security requirements. This project will also improve DMHC security posture by removing the need to rely on end-users to manage multiple account credentials with single sign-on capability.

TIP: Copy and paste or click the + button in the lower right corner to add Business Programs, with background and context and impact descriptions as needed.

1.6 Project Justification

1. **Strategic Business Alignment**

Enterprise Architect

Title: Enterprise Architect

Name: Vijay Mopuru

Strategic Plan Last Updated? 4/29/2020

Strategic Business Goal: Foster a culture of excellence throughout the organization

Alignment: This project will enable the use of all resources effectively, efficiently, and securely. It will also ensure that the organization can respond effectively and in a timely manner to all unexpected events.

TIP: Copy and paste or click the + button in the lower right corner to add Strategic Business Goals and Alignments as needed.

Mandate(s): None

Bill Number/Code, if applicable: None

Add the Bill language that includes system-relevant requirements:

Not Applicable

TIP: Copy and paste or click the + button in the lower right corner to add Bill Numbers/Codes and relevant language as needed.

2. **Business Driver(s)**

Financial Benefit: No

Increased Revenue: No

Cost Savings: Yes

Cost Avoidance: No

Cost Recovery: No

Will the state incur a financial penalty or sanction if this proposal is not implemented? No

If the answer to the above question is “Yes,” please explain:

Click or tap here to enter text.

Improvement

Better Services to the People of California: Yes

Efficiencies to Program Operations: Yes

Improved Equity, Diversity, and/or Inclusivity: No

Improved Health and/or Human Safety: No

Improved Information Security: Yes

Improved Business Continuity: Yes

Improved Technology Recovery: Yes

Technology Refresh: No

Technology End of Life: No

1.7 Business Outcomes Desired

Executive Summary of the Business Problem or Opportunity:

The Office of Technology and Innovation (OTI) is currently maintaining six public-facing web portals that require authentication. Being managed within these portals are 17 applications and about 11,000 external user accounts. The authentication technology used by these portals is outdated and prevents the DMHC from swiftly meeting application-related security mandates. It continues to pose a limit in DMHC's technology modernization initiatives due to integration difficulties with modern cloud platforms. In on-going operations, the current system design requires an individual to have a separate account for each organization he/she represents. This dependency on external users to securely manage many account credentials increases security risks in DMHC systems.

The OTI seeks to enhance the existing IDAM to lay the foundation for application modernization, reduce security risks, and achieve versatility in addressing security threats. The updated IDAM would provide one intuitive and accessible user interface (UI) that consolidates siloed portals and data. This centralized UI would reduce technology debt and increase maintenance efficiency for the OTI by not having to manage six different portals. The Department would be able to provide a Single Sign-on experience with one account dataset, resulting in operational efficiency and improved security with less credential issues from external users. Finally, the modern technology that comes with the updated IDAM would permit seamless integration with latest cloud technologies and accelerates the DMHC's application modernization effort.

Objective ID: 1

Objective: Improve user experience by implementing single sign-on capabilities.

Metric: Number of users having more than one account

Baseline: 1608 users have multiple accounts, for a total of 6351 accounts

Target Result: 50% reduction in the number of users who have multiple accounts in 6 months after implementation of the new IDAM platform. This will be measured by generating a user account report from the system.

Objective ID: 2

Objective: Improve information security by providing modern accessible user interface that is compliant with industry best practices for web accessibility and security.

Metric: Number of non-compliant issues – example non-compliance with latest version of the Web Content Accessibility Guideline (WCAG)

Baseline: 60 critical issues across six public-facing existing portals

Target Result: 0 critical issues across six public-facing existing portals within 6 months of implementation. This will be measured by conducting an audit of the six public facing portals, using tools to validate the WCAG compliance, to determine the number of critical issues.

Objective ID: 3

Objective: Increase efficiencies to program operations by reducing the time to develop, modify and integrate application security features between platforms.

Metric: Number of hours to develop and integrate a new security feature across platforms

Baseline: 6 months (1000 hours) to add a new security feature across platforms

Target Result: Within 3 months of implementation, 50% reduction in time to add new security features across 6 platforms. This will be measured by the start and end date of the integration of the application security features between platforms.

Click or tap here to enter text.Click or tap here to enter text.Click or tap here to enter text.

TIP: Copy and paste or click the + button in the lower right corner to add Objectives as needed. Please number for reference.

TIP: Objectives should identify WHAT needs to be achieved or solved. Each objective should identify HOW the problem statement can be solved and must have a target result that is specific, measurable, attainable, realistic, and time-bound. Objective must cover the specific. Metric and Baseline must detail how the objective is measurable. Target Result needs to support the attainable, realistic, and time-bound requirements.

1.8 Project Management

1. **Project Management Risk Score:** 0.6

   Follow the instructions in Statewide Information Management Manual (SIMM) Section 45 Appendix B Project Management Risk Assessment Preparation Instructions.

   Attach a completed Statewide Information Management Manual (SIMM) Section 45 Appendix A Project Management Risk Assessment Template to the email submission.

2. **Project Approval Lifecycle Completion and Project Execution Capacity Assessment**

   Does the proposal development or project execution anticipate sharing resources (state staff, vendors, consultants, or financial) with other priorities within the Agency/state entity (projects, PALs, or programmatic/technology workload)?

   Answer: Yes

   Does the Agency/state entity anticipate this proposal will result in the creation of new business processes or changes to existing business processes?

   Answer (No, New, Existing, or Both)**:** Both New and Existing Processes

1.9 Initial Complexity Assessment

1. **Complexity Assessment (Business Score):** Business Complexity: 0.7; Technical Complexity: 1.2

   Follow the instructions in the Statewide Information Management Manual (SIMM) Section 45 Appendix D Complexity Assessment Instructions.

   Attach a completed Statewide Information Management Manual (SIMM) Section 45 Appendix C Complexity Assessment Template to the email submission.

   NOTE: Business complexity is initially completed in PAL Stage 1. Technical complexity is initially completed in PAL Stage 2.

2. **Noncompliance Issues:** Indicate if your current operations include noncompliance issues and provide a narrative explaining how the business process is non-compliant.

   Programmatic regulations: No

   HIPAA/CIIS/FTI/PII/PCI: No

   Security: No

   ADA: Yes

   Other: No

   Not Applicable: No

Noncompliance Description:

Six external facing application portals are not fully compliant with critical accessibility requirements imposed by AB434.

3. **Additional Assessment Criteria**

If there is an existing Privacy Threshold Assessment/Privacy Information Assessment, include it as an attachment to your email submission.

How many locations and total users is the project anticipated to affect?

Number of locations: Statewide across California

Estimated Number of Transactions/Business Events (per cycle): Click or tap here to enter text.

Approximate number of internal end-users: 150

Approximate number of external end-users: 12,965

1.10 Funding

Planning

1. Does the Agency/state entity anticipate requesting additional resources through a budget action to ***complete planning*** through the project approval lifecycle framework? Yes

If Yes, when will a budget action be submitted to your Agency/DOF for planning dollars?

9/3/2024

2. Please provide the Funding Source(s) and dates funds for planning will be made available:

Managed Care Fund via BCP – available 07/01/2025 (Submit Fall 2024 BCP for FY 2025-2026)

Project Implementation Funding

1. Has the funding source(s) been identified for ***project implementation***? Yes

If known, please provide the Funding Source(s) and dates funds for implementation will be made available:

Managed Care Fund via BCP – available 07/01/2026

Will a budget action be submitted to your Agency/DOF? Yes

If “Yes” is selected, specify when this BCP will be submitted: September 2025 (Submit a Fall 2025 BCP for FY 2026-2027)

2. Please provide a rough order of magnitude (ROM) estimate as to the total cost of the project: Less than $10 Million

End of agency/state entity document.

Please ensure ADA compliance before submitting this document to CDT.

When ready, submit Stage 1 and all attachments in an email to ProjectOversight@state.ca.gov.

Department of Technology Use Only

Original “New Submission” Date: 09/17/2024.

Form Received Date: 09/17/2024.

Form Accepted Date: 09/17/2024.

Form Status: Completed

Form Status Date: 09/17/2024.

Form Disposition: Approved.

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

Form Disposition Date: 09/17/2024

Department of Technology Project Number (0000-000): 4150-036