WORK ORDER 19 – BenefitsCal NIST SP 800-53 Rev. 5 Initiatives

Cal**SAWS** BenefitsCal (Portal/Mobile) Work Order

Table of Contents

1.0 Work Order Submission & Approval Form

Work Order Number	19
Work Order Title	BenefitsCal NIST SP 800-53 Rev. 5 Initiatives
Submitted Date	7/18/25
Originator	California Department of Social Services (CDSS) and Department of Health Care Services (DHCS) Request
Priority	Select the estimated priority level of the requested Work Order: ☐ Critical – is necessary to avoid potential project stoppage. ☐ High – is necessary to avoid potential significant impact to the goals and objectives of the project. ☒ Medium – is necessary to avoid potential impact to the operational efficiency of project execution. ☐ Low – needs to be addressed, but the estimated impact to the project is minimal.
Detailed Description	This Work Order includes four initiatives to mature the BenefitsCal Security and Privacy framework to meet Revision 5 controls from NIST SP 800-53. The following are the initiatives included in this Work Order: • Project 1 – PII Processing and Management: Design and pilot a SaaS-based Data Security Posture Management (DSPM) platform that continuously discovers, classifies, and tracks sensitive data across BenefitsCal AWS accounts. Upon successful pilot, complete an implementation of the DSPM platform. Develop and configure the DSPM use cases and policies to adhere to NIST SP 800-53 for monitoring least-privilege access, encryption, and data-retention. Success involves integration of DSPM with BenefitsCal AWS accounts so that sensitive data is accurately classified and protected. • Project 2 – Security Monitoring: Enable AWS Security Lake for central security audit event collection and normalization. Ingest CloudTrail, VPC Flow Logs, and other audit event sources into the AWS Security Lake. Enable and configure AWS Detective to consume Security Lake data, analyze events, and provide investigation capabilities. Refactor existing application logging in CloudWatch to minimize personally identifiable information. Support integration of the BenefitsCal AWS Security Lake with the CalSAWS SIEM solution. • Project 3 – System Security Plan (SSP) and Operational Working Document (OWD) Updates: Perform control-gap analysis between

	the Revision 4 approved SSP and Revision 5 baseline, develop or update SSP control responses for new or changed controls, publish the SSP in the new GRC platform. Review and update OWDs that support the procedural controls of the SSP. • Project 4 – Supply Chain Risk Management Controls: Develop a Supply Chain Risk Management (SCRM) Plan. Establish processes to address supply chain weaknesses, and document supply chain controls and processes. Create OWD for SCRM control family.	
Review Date		
Type of Work Order	☐ Fixed Fee	▣ Time & Material

2.0 Work Order Impact Analysis

Describe the changes required to support this Work Order by resource type and provide a brief description of work to be completed.

Design Impact	• None – changes do not affect the frontend of the BenefitsCal application.

Development	• Project 1 – PII Processing and Management:
	  ○ None – changes do not require custom development.
	• Project 2 – Security Monitoring:
	  ○ Refactor logging methods to log Lambda function execution logs in database instead of CloudWatch.
	• Project 3 – SSP and OWD Updates:
	  ○ Provide input on architecture and data flow designs.
	• Project 4 – Supply Chain Risk Management Controls:
	  ○ None – changes do not require custom development.

Testing	• Project 1 – PII Processing and Management:
	  ○ Testing of DSPM policies using sample PII datasets.
	• Project 2 – Security Monitoring:
	  ○ Validate log ingestion completeness.
	• Project 3 – SSP and OWD Updates:
	  ○ Control assessment to be performed as part of the SSP update.
	• Project 4 – Supply Chain Risk Management Controls:
	  ○ None – changes do not require testing.

Performance Testing	• None – the frontend and backend services for BenefitsCal will not be impacted by the integrations.
Training	• None – no external training is necessary for these initiatives.
Communications	• None – no external involvement is needed for communications.

Security	• Project 1 – PII Processing and Management:
	  ○ Implement DSPM and configure policies to comply with NIST SP 800-53. Perform data discovery scans. Review and analyze results from DSPM scans. Collect evidence of compliance.
	• Project 2 – Security Monitoring:
	  ○ Enable and provision AWS Security Lake, including ingestion of the AWS logs. Enable and configure AWS Detective for analytics of AWS data sources. Create and document incident response processes for using Security Lake and Detective.
	• Project 3 – SSP and OWD Updates:
	  ○ Prepare updated authorization boundary, network, and data flow diagrams as part of the Rev. 5 narrative.

	Complete responses to selected SSP controls and update supporting OWDs. • Project 4 – Supply Chain Risk Management Controls: ○ Develop a Supply Chain Risk Management (SCRM) Plan. Establish processes to address supply chain weaknesses, and document supply chain controls and processes. Create OWD for SCRM control family.

Software/Licenses	• Project 1 – PII Processing and Management:
	  ○ Procure subscription for a DSPM
	• Project 2 – Security Monitoring:
	  ○ Allocate budget for AWS costs for AWS Security Lake and Detective
	• Project 3 – SSP and OWD Updates:
	  ○ None
	• Project 4 – Supply Chain Risk Management Controls:
	  ○ None

Deliverables (New and Updated)	• New DEL PII Processing and Management Report • New DEL Security Monitoring Implementation Report • Updated BenefitsCal System Security Plan and associated OWDs • New OWD Supply Chain Risk Management Procedures
Schedule	• None – these initiatives do not impact the BenefitsCal release schedule
Other	• None

Assumptions	• Project 1 – PII Processing and Management:
	  ○ The initiative will start with a design and pilot to validate the compatibility and capability of the selected Data Security Posture Management platform. Following the pilot will be the implementation of the identified and approved use cases to meet the NIST SP 800-53 Rev. 5 requirements.
	  ○ BenefitsCal teams will implement and manage the Data Security Posture Management platform.
	• Project 2 – Security Monitoring:
	  ○ Scope only includes existing security audit log events being ingested into Security Lake.
	• Project 3 – SSP and OWD Updates:
	  ○ SSP will be updated in the template shared by the Consortium Security team.
	  ○ SSP will be submitted through iterative submissions each month and a formal submission in January 2026 as per the Consortium Security's schedule.

	○ SSP controls that are BenefitsCal's responsibility have been identified and reviewed with the Consortium Security as part of the SSP scoping activity. • Project 4 – Supply Chain Risk Management Controls: ○ BenefitsCal SCRM process will follow the Consortium Security's guidelines for SCRM, including use of Consortium selected platform.

2.1 Work Order Hours / Fees

2.1.1 Estimated hours required to support this Work Order (**Project 1 – PII Processing and Management**) by resource type and provide a brief description of work to be completed, if applicable summarized below:

Type	Description	Rate	Hours	Amount
Executive SM	Security Lead	$181.17	510	$92,396.70
Engagement PM	Senior Security Engineer	$148.23	800	$118,584.00
Data Privacy Specialist	Senior Security Engineer	$148.23	480	$71,150.40
Data Privacy Specialist	Security Engineer	$142.74	800	$114,192.00
Data Privacy Specialist	Security Engineer	$142.74	480	$68,515.20
Data Privacy Specialist	Security Engineer	$142.74	480	$68,515.20
			Total	$533,353.50

2.1.2 Estimated hours required to support this Work Order (**Project 2 – Security Monitoring**) by resource type and provide a brief description of work to be completed, if applicable summarized below:

Type	Description	Rate	Hours	Amount
Engagement PM	Security Lead	$181.17	250	$45,292.50
Data Privacy Specialist	Senior Security Engineer	$148.23	800	$118,584.00
Data Privacy Specialist	Senior Security Engineer	$148.23	800	$118,584.00
DevOps Specialist	DevOps/Tools Engineer	$91.13	800	$72,904.00
Developer	Junior Programmer Analyst	$109.80	400	$43,920.00
Developer	Junior Programmer Analyst	$109.80	400	$43,920.00

Total	$443,204.50

2.1.3 Estimated hours required to support this Work Order (**Project 3 – SSP and OWD Updates**) by resource type and provide a brief description of work to be completed, if applicable summarized below:

Type	Description	Rate	Hours	Amount
Engagement PM	Security Lead	$181.17	200	$36,234.00
Security Compliance Lead	Senior Security Engineer	$148.23	800	$118,584.00
Security Compliance Specialist	Senior Security Engineer	$148.23	800	$118,584.00
Privacy Specialist	Security Engineer	$142.74	800	$114,192.00
Privacy Specialist	Security Engineer	$142.74	480	$68,515.20
			Total	$456,109.20

2.1.4 Estimated hours required to support this Work Order (**Project 4 – Supply Chain Risk Management Controls**) by resource type and provide a brief description of work to be completed, if applicable summarized below:

Type	Description	Rate	Hours	Amount
Engagement PM	Security Lead	$181.17	275	$49,821.75
Security Specialist	Senior Security Engineer	$148.23	800	$118,584.00
Security Specialist	Senior Security Engineer	$148.23	800	$118,584.00
Security Specialist	Security Engineer	$142.74	320	$45,676.80
			Total	$332,666.55

2.2 Payment Schedule (If Applicable)

Payment Point	Description	Milestone Date	WAC Date	Invoice Submission Date	Cost
Project 1: Design and Pilot of DSPM platform	Completion of the eight-week design and pilot activities.	09/26/2025	10/26/2025	10/31/2025	$98,545.50
Project 1: Data Security Posture Management Platform	Software for DSPM – pending approval by the Consortium	09/26/2025	-	-	Not to Exceed $125,000
Project 1: Submission of DEL PII Processing and Management Report	Submission of Deliverable associated to the Project 1.	12/30/2025	01/30/2026	01/31/2026	$434,808.00
Project 2: Delivery of the following CSPMs in Production: • CSPM-79873 Phase 1: Migration of AWS CloudWatch payload to BenefitsCal DB • CSPM-79874 Phase 2: Update APIs Interacting with Partner Interfaces • CSPM-79875 Phase 3: Update First Set of Non-Partner Facing APIs • CSPM-79876 Phase 4: Update Remaining Non-Partner Facing APIs	Delivery of the code changes to BenefitsCal Production	10/24/2025	11/24/2025	11/30/2025	$87,840.00

Project 2: Submission of DEL Security Monitoring Implementation Report	Submission of Deliverable associated to the Project 2.	12/30/2025	01/30/2026	01/31/2026	$355,364.50
Project 3: Submission of DEL System Security Plan	Submission of Deliverable associated to the Project 3.	12/30/2025	01/30/2026	01/31/2026	$456,109.20
Project 4: Submission of OWD Supply Chain Risk Management Procedures	Submission of Deliverable associated to the Project 4.	12/30/2025	01/30/2026	01/31/2026	$332,666.55

Invoice submissions require WAC and approval from the Consortium. The milestone date, the WAC date and the invoice submission date will need Consortium agreement.

Deliverables listed below will be provided to support this Work Order and, upon approval of the Work Order, are considered to be part of **Section 5.2 – Portal/Mobile App Deliverables and Services.**

#	Deliverable Title	Description	Deliverable Submission Date
1	DEL PII Processing and Management Report	This report will cover the identification, documentation, and monitoring of Personally Identifiable Information (PII) data across BenefitsCal system components.	12/30/2025
2	DEL Security Monitoring Implementation Report	This report will provide a detailed account of the security monitoring measures implemented, their effectiveness, and the use cases designed for monitoring.	12/30/2025
3	DEL System Security Plan	The System Security Plan will be updated to address the Revision 5 controls of the NIST SP 800-53 framework.	12/30/2025

4	OWD Supply Chain Risk Management Procedures	The OWD will document the process implemented for managing the Supply Chain Risk for BenefitsCal.	12/30/2025

2.3 Consortium Responsibilities

If applicable, specify work(s) which will be supported by the Consortium for this Work Order.

Work	Work Description
	• Review and approve deliverable updates.

3.0 Work Order Execution

IN WITNESS WHEREOF, the Consortium has caused this Work Order to be subscribed on behalf of the Consortium and Contractor has caused this Work Order to be subscribed on its behalf by its duly authorized officer, as indicated below.

DELOITTE CONSULTING LLP

Dated: _____

By: _____

Name: Rachel Frey

Title: Deloitte Principal

CALSAWS CONSORTIUM

Dated: _____

By: _____
Michael Sylvester, Consortium Chair

By: _____
Kronick Moskovitz Tiedemann & Girard,
Consortium Legal Counsel

By: _____
Julia Erdkamp, Consortium Executive Director