CLEARBEST

Change Order No. 4 – Security Review Plan and Quarterly Report Requirements Update

Purpose

The purpose of this Change Order is to update certain subparts of two (2) requirements of QA Deliverable #9 – QA Security Review Plan and QA Deliverable #10 – Quarterly QA Security Reports to align with current industry standards and guidelines for information technology security, and to correct the cadence of QA Security Report from monthly to quarterly. This Change Order does not impact the Cost of the Agreement between the Consortium and ClearBest and does not otherwise alter, amend, or revise that Agreement, except as expressly set forth in this Change Order.

Scope

The following provide updates to the Security Review Plan and Quarterly QA Security Report requirements.

Req ID		Category	Original Requirement	Revised Requirement	Reason for Change
SR	69	Deliverable	The QA Vendor shall provide a **Security Review Plan** prior to the Initial M&O period that includes, at a minimum, the following information:		
			A. Scope of security reviews and audits (CalSAWS Systems);		
			B. Approach to conduct security reviews and audits including, but not limited to:		
			a. Recommended Security Controls for Federal Information Systems (National Institute of Standards and Technology (NIST), Special Publication 800-53;		
			b. Standards for Security Categorization of Federal Information and Information Systems (Federal Information and Processing Standards (FIPS) Publication 199);		

Req ID	Category	Original Requirement	Revised Requirement	Reason for Change
		c. Security Requirements for Cryptographic Modules (FIPS Publication 140-2)		
		d. Minimum Security Requirements for Federal Information and Information Systems (FIPS Publication 200)		
		e. Automatic Data Processing Physical Security and Risk Management (FIPS, Publication 31)	e. Guide for Conducting Risk Assessments (SP 800-30, Rev. 1)	Updated Item SR69.B.e to reference the most current publication as the Guide for Conducting Risk Assessments (SP 800-30, Rev. 1) supersedes FIPS, Publication 31.
		f. Computer Security Guidelines for Implementing the Privacy Act of 1974 (FIPS, Publication 41)	Remove	Removed Item SR69.B.f. as the Computer Security Guidelines for implementing the Privacy Act of 1974 (FIPS, Publication 41) has been retired by the Industry.
		g. Guidelines for Security of Computer Applications (FIPS, Publication 73)	Remove	Remove Item SR69.B.g. as the Guidelines for Security of Computer Applications (FIPS, Publication 73) has been retired by the Industry.
		h. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 and the associated Standards for Privacy of Individually Identifiable Health Information		

Req ID		Category	Original Requirement	Revised Requirement	Reason for Change
			C. Vendor roles and responsibilities for security reviews;		
			D. Processes for managing security reviews such as, listing specific security breaches by DD&I Vendor by specific provisions, reporting methodology and timing, and recommending solutions to breaches;		
			E. Processes for identifying potential areas of security risk and reporting of potential solutions;		
			F. Product comparisons to specifications, industry standards and best practices, and provide assessments to the Consortium Project Management Team;		
			G. Identification of security standards and industry best practices to be used in reviews and in comparison, for reporting; and		
			H. Monthly reporting methodology for communicating:	Quarterly reporting methodology for communicating:	Updated SR69.H to correctly read "Quarterly" instead of "Monthly" to align with the required quarterly reporting.
			a. Security related incidents;		
			b. Deficiencies;		
			c. The extent to which the Vendor is meeting its obligations;		
			d. Whether the Vendor is in breach;		
			e. How to mitigate the impact to the Consortium and/or Counties; and		

Req ID		Category	Original Requirement	Revised Requirement	Reason for Change
			f. How the Vendor should cure its breach including timelines.		
SR	70	Deliverable	The QA Vendor shall provide a **Quarterly QA Security Report** that includes, at a minimum, the following:		
			A. Executive Summary (Both MS Word and MS PowerPoint formats);		
			B. Reporting Period;		
			C. Date of Report;		
			D. Summary of Security Activities Completed;		
			E. Summary of Security Activities in Process;		
			F. Summary of Security Activities Scheduled for this Period that were not Completed and the reasons they were not completed;		
			G. Summary of Security Activities Scheduled for the upcoming report period;		
			H. Detailed description(s) of Security Related Incidents in accordance with the Security Review Plan including Vendor response, mitigation plans;		
			I. Security Issues;		
			J. Security Risks;		
			K. Recommendations; and		
			L. Other pertinent information.		
			The **Quarterly QA Security Reports** should begin after the first full month following the initial CalSAWS implementation and the start of the Initial M&O Phase.		
			The **Quarterly QA Security Report** must be submitted within 5 business days after the completion of a month.	The **Quarterly QA Security Report** must be submitted within 5 business days after	Updated SR70 to correctly read "quarter" instead of "month" to align

Req ID	Category	Original Requirement	Revised Requirement	Reason for Change
			the completion of a quarter.	with the required quarterly reporting.

Timeframe

Implement as part of the development and approval of the Security Review Plan and remain in place through the regular delivery of the Quarterly QA Security Reports.

Staffing and Costs

No changes to staffing or costs.

Change Order Approval

IN WITNESS WHEREOF, the Parties have set their hands hereunto as of the Execution Dates set forth below.

CalSAWS Consortium

By:_____
Printed Name: Michael Sylvester
Title: Board Chair
Date: _____

ClearBest, Incorporation

By:_____
Printed Name: Wendy Battermann
Title: President
Date: _____

CalSAWS Consortium

By:_____
Printed Name: John Boule
Title: Executive Director
Date: _____

APPROVED AS TO FORM:

_____
Jeff Mitchell
Consortium Legal Counsel