CLEARBEST

Change Order No. 8 Work Order No. 5: NIST/Zero-Trust/Upgrades QA Services

The purpose of this Work Order is to outline the scope, timeframe, staffing, and costs to perform Quality Assurance Services for the NIST/Zero-Trust/Upgrades occurring between June 1, 2024, through May 31, 2026.

Scope

The NIST/Zero-Trust/Upgrades are complex efforts that include multiple, different activities. Detailed descriptions of these activities are provided in the CalSAWS January 2024 As-Needed IAPDU Narrative, dated May 3, 2024. The following is a summarized version of the IAPDU descriptions:

1. Hardening of the CalSAWS solution to align with Zero-Trust Architecture (ZTA) principles has been identified as critical to the ongoing security and protection of CalSAWS. Several improvements have been identified in the following key areas:
   A. Network Migration
   B. Network Test Lab
   C. Deploy Edge Firewalls
   D. Strong Authentication
   E. BenefitsCal – Identity and Access Management
   F. BenefitsCal – AWS Monitoring, Analytics, and Thread Response
2. CalSAWS compliance with NIST Revision 5 updates is imperative to the overall security framework of the platform. CalSAWS is currently in compliance with Revision 4, but additional standards that have been added to Revision 5. These additional standards are important guidelines to organizations like CalSAWS to maintain the necessary levels of security to continually address patterns used by cyber criminals to access technology platforms. The NIST Uplift effort includes:
   A. Splunk Risk Based Alerting
   B. ServiceNow IT Operational Management (ITOM)
   C. Supply Chain Risk Management Controls
   D. Identify Password Authentication
   E. AppSec Scanning Upgrade
   F. AWS Macie
   G. Microsoft Purview Data Security
   H. Identity Proofing
   I. System Security Plan (SSP)/Organization Defined Parameters
   J. Non-Implementation / Process Change Roll-Out
   K. Split Tunneling Enablement
   L. Technology Initiatives to meet Security Control Requirements
   M. Additional Security and Privacy Process & Procedural Updates
3. Additional security features, which are supplemental to the Zero-Trust and NIST Revision 5 upgrades. The following is a summary list of the items that are described in detail in the IAPDU:
   A. Tenant Configuration
   B. Office 365 Services Backup Solution

C. Cloudfront Integration
D. AWS API Developer Portal
E. Third-Party Cookies Phase Out
F. Enhanced Email Message Examination
G. Migration Production Accounts to TFC Managed Account
H. Intune Mobile and Modern Device Management
I. Splunk SVC Uplift for Vendor Logs
J. Replace Physical Equinix hosted BigIP F5 with Next Generation Hardware
K. Update Virtual BigIP F5 with NGFW at Partner Exchange & Network Prod Account
L. Redundant Solarwinds
M. Redundant Syslog Setup
N. Center for Internet Security (CIS) Partition

4. The Consortium has identified several major hardware and software upgrades required as part of its technical roadmap. Minor upgrades are accounted for in baseline technical infrastructure hours and costs, but several major products are coming to end of life or have newer versions that must be aligned to. CalSAWS is required to stay within one version of the most recent release (N-1) to ensure continuity of support and avoid security vulnerabilities. These updates require changes to the application, extensive regression testing, and updates to configurations. The following provides a summary list of the items that are described in detail in the IAPDU:

   A. Upgrade Nodejs Lambdas to Version 22+
   B. Migrate Spectrum UAM Loqate to Global Addressing Module (GAM))
   C. Upgrade Spring Version
   D. Upgrade SpringBoot APIs
   E. Upgrade CalSAWS Libraries to be N-1 Compliant
   F. Upgrade ODM (Operational Decision Manager) Rules Engine to Version 8.12
   G. OS Upgrade - Cisco Routers/Switches/Firewalls
   H. Replace TPX SD-WAN (Routers & Virtual Firewall) and TPX Adtran EOL Switches
   I. Analytics Stack (EMR Upgrade, Python Upgrade and Qlik and Nprinting Upgrade)
   J. Win11 Migration
   K. Upgrade to WinSrvr 2025
   L. Upgrade Windows 2016/2019 Servers to Windows 2022
   M. RDS Upgrade
   N. ForgeRock - Major version upgrade
   O. Red Hat EL OS Upgrade
   P. Amazon Linux 3 Upgrade
   Q. DevSecOps Tools Upgrade
   R. Lobby Management Integration
   S. Lobby Monitor Updates

ClearBest will provide QA support to the Consortium throughout the implementation of the NIST/Zero-Trust/Upgrades in alignment with the above-listed activities. QA Services include monitoring, guiding, and confirming that the NIST/Zero-Trust/Upgrades are completed without disrupting the stability of normal business operations and system availability. In general, NIST/Zero-Trust/Upgrades will include:

1. Participating in meetings, discussions, and walkthroughs pertaining to the NIST/Zero-Trust/Upgrades activities, deliverables, work products, and milestones.

2. Monitoring overall enhancement progress and schedules.
3. Reviewing NIST/Zero-Trust/Upgrade activities and outcomes to validate that:
   A. Production Readiness checklists are thorough and have been completed.
   B. Implementation processes and procedures are being followed and appropriate communications/training materials are generated where there is an identified user impact as a result of the change.
4. Reviewing Additional Security Features to validate that:
   A. Readiness and other pertinent checklists are thorough and have been completed.
   B. Implementation processes and procedures are being and appropriate communications/training materials are generated where there is an identified user impact as a result of the change.
   C. Findings are resolved.
5. Reviewing Other Technical Upgrades to validate that:
   A. Agreed upon requirements are being met and tracked.
   B. Readiness and other pertinent checklists are thorough and have been completed.
   C. Implementation processes and procedures are being followed and risks/issues are escalated timely.
   D. Risks, issues, and changes are being effectively managed within the appropriate Risk/Issue register.
   E. Findings are resolved.
6. Reviewing and execution Testing and Validation activities and outcomes to integrate QA testing plans and validate that:
   A. Testing and validation requirements are being met and tracked.
   B. The contractors are executing NIST/Zero-Trust Validation Plan, as stated.
   C. Verify that The Validation Plan for Additional Security Features and Other Technical Upgrades is being executed.
   D. The NIST/Zero-Trust, additional security features, and other technical upgrades meet requirements and are ready for production.
   E. Outcomes are accurate and reported as planned and communication for problems and corrective actions is timely.
   F. Review user communications and training materials to ensure necessary information about changes that impact users are distributed.

   The QA Test team will conduct Independent Testing and Validation for mission-critical, high-priority, and functionally complex changes.
7. Reporting on QA activities, findings, and recommendations from the assessment of NIST/Zero-Trust/Upgrades as part of Deliverable #76 – NIST/Zero-Trust/Upgrades Status Report. Content of Deliverable #76 will be included within the Deliverable #65 – QA Status Report.
8. Reporting on QA findings at the CalSAWS Weekly Status Meetings, Project Steering Committee (PSC), Joint Powers Authority (JPA) Board Meetings, and other stakeholder meetings as required.

9. Support CalSAWS vendors in writing and submitting quality and compliant deliverables, work products, and system security plan responses specific to Zero Trust and NIST rev 5 changes.
10. Review vendor and system scope to ensure comprehensive system security plans and control responses for Zero Trust and NIST rev5.
11. Provide project-level recommendations and status updates for compliance and deliverable documentation across all vendors and in-scope systems to Consortium Security on a monthly basis
12. Review POAM status changes for Zero Trust and NIST rev5 quality and compliance.

Staffing and Cost

To perform the NIST/Zero-Trust/Upgrades, ClearBest is assigning resources based on the level of effort to complete the tasks outlined in the Scope section. The estimated effort for the NIST/Zero-Trust/Upgrades is as follows:

QA Staff Role	Hours	Rate	Cost
QA Technical Lead	9,120	$139	$1,267,680
Total	**9,120**		**$1,267,680**

Costs by Deliverable and SFY

The cost schedules to support the QA Services associated with the NIST/Zero-Trust/Upgrades have been incorporated into the Quality Assurance Project Cost Schedules and are attached. The total cost of Change Order 8, Work Order 5 will not exceed $1,267,680. The monthly deliverable cost for SFY 24/25 is estimated to be $72,785.50. The monthly deliverable cost for SFY 25/26 is estimated to be $38,920.00. The following provides the not-to-exceed total costs by deliverable and SFY:

SERVICE	SFY 24/25	SFY 25/26	TOTAL
DEL #76 - QA NIST/Zero-Trust/Upgrades MSR	$800,640	$467,040	$1,267,680
TOTAL	**$800,640**	**$467,040**	**$1,267,680**

Work 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: Julia Erdkamp
Title: Executive Director
Date: _____

APPROVED AS TO FORM:

By: _____
Jeff Mitchell
Consortium Legal Counsel
Date: _____