

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER 21-10459	PURCHASING AUTHORITY NUMBER (If Applicable)
------------------------------	---

1. This Agreement is entered into between the Contracting Agency and the Contractor named below:

CONTRACTING AGENCY NAME

California Department of Public Health

CONTRACTOR NAME

Deloitte Consulting LLP

2. The term of this Agreement is:

START DATE:

September 16, 2021 or upon CDPH approval, whichever is later

THROUGH END DATE

September 15, 2022

3. The maximum amount of this Agreement is:

\$800,000

Eight Hundred Thousand Dollars and Zero Cents

4. The parties agree to comply with the terms and conditions of the following exhibits, which are by this reference made a part of the Agreement.

Exhibits	Title	Pages
Attachment 1	Statement of Work	12
Attachment 2	Agency Special Provisions	3
Attachment 2A	Cost Worksheet	1
Attachment 2B	Invoice Format (Sample)	1
Attachment 2C	Work Order Authorization (Sample)	2
Attachment 3	Information Technology General Provisions (GSPD-401 IT)	12
Attachment 4	Resumes	13
Attachment 5	FEMA Provisions	5
Attachment 6	Contractor's Release	1
Attachment 7	CDPH HIPAA BAA	14
Attachment 8	CDPH ISO/SR1	21

Items shown with an asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto.

These documents can be viewed at <https://www.dgs.ca.gov/OLS/Resources>

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER

21-10459

PURCHASING AUTHORITY NUMBER (If Applicable)

IN WITNESS WHEREOF, THIS AGREEMENT HAS BEEN EXECUTED BY THE PARTIES HERETO.

CONTRACTOR

CONTRACTOR NAME (If other than an individual, state whether a corporation, partnership, etc.)

Deloitte Consulting LLP

CONTRACTOR BUSINESS ADDRESS 555 Mission Street	CITY San Francisco	STATE CA	ZIP 94105
PRINTED NAME OF PERSON SIGNING Christine Huddleson	TITLE Managing Director		
CONTRACTOR AUTHORIZED SIGNATURE Huddleson, Christine Wight (US - Sacramento)	DATE SIGNED 9/15/2021		

STATE OF CALIFORNIA

CONTRACTING AGENCY NAME

California Department of Public Health

CONTRACTING AGENCY ADDRESS 1616 Capitol Avenue, MS 1802	CITY Sacramento	STATE CA	ZIP 95814
PRINTED NAME OF PERSON SIGNING Kristy Lieu	TITLE Chief, Contract Management Unit		
CONTRACTING AGENCY AUTHORIZED SIGNATURE 	DATE SIGNED 9/15/21		
CALIFORNIA DEPARTMENT OF GENERAL SERVICES APPROVAL		EXEMPTION (If Applicable) Executive Order N-25-20	

ATTACHMENT 1 **STATEMENT OF WORK**

1. STATEMENT AND DESCRIPTION

The Contractor agrees to provide the California Department of Public Health (CDPH) the services described herein. This Statement of Work (SOW) reflects the services the Contractor shall provide to CDPH. The Offeror must have extensive and demonstrated technical knowledge and experience as identified in this SOW.

In response to the Governor's Proclamation of a State of Emergency dated March 4, 2020, and Executive Order N-25-20, due to current public health emergencies, the CDPH has determined that CDPH must take immediate action.

Since March 2020, reliance on several existing CDPH systems became critical due to COVID-19. New systems were deployed, and existing ones upgraded rapidly to meet demands. Existing systems were not designed to handle the transaction types and increased volumes resulting from COVID 19 and experienced critical performance issues. These systems were relied upon to track cases, deaths, testing, contact trace, and monitor population vaccination information. With the high numbers of confirmed cases, deaths, tests, and vaccinations, the systems were critical and system failures made the job of addressing the urgent needs especially challenging. These systems are generally used for other purposes as well. For example, the California Immunization Information System was originally designed to house all immunizations for providers to voluntarily leverage and query against, but now it's used as the source data for all COVID vaccine reporting and verification.

To support these technology assets and continue to provide effective services to all Californians, state departments, and programs CDPH requires the services of a Contractor that has the industry expertise. Which will be necessary to perform technical application, platform, and infrastructure assessments to identify gaps, issues, and potential areas of vulnerability to be addressed and recommend strategies that will allow CDPH to continue to provide highly resilient and stable services critical to combating COVID-19.

The primary goal is for CDPH to improve the stability and resiliency of the technical ecosystems. Our goal is to ensure architectural components are holistically implemented and that they provide continuity of mission essential functions and services during any type of disruption. To achieve this goal CDPH needs to understand the health of components in the technical ecosystem, their current business value, their likely impact on future business value, and the business exposure due to technical condition.

The purpose of this contract is to obtain specialized expertise to perform a capability assessment of the complex CDPH technical ecosystems, and the end user experience provided through the underpinning services and technical stack. This assessment focuses on the availability and stability of applications, systems, platforms, services, and infrastructure which ensure the continuity of business operations and services. Areas of assessment include but not limited to architecture alignment, system management, security, support (Contractor and State staff),

maintainability, performance, and scalability. Outcomes of the assessment are identified vulnerabilities, risks, and stabilization opportunities.

The work products and outputs from the assessment will be in the form of a comprehensive report that provides major findings on the current-state technology ecosystem that includes the human aspect, automation monitoring, architecture, end to infrastructure service and information stack, core central services, prioritization / classification of mission critical applications, service support (problem and change management), and root cause analysis. As well as recommendations, short-term, intermediate, and long-term strategies, and roadmaps necessary to remediate and build a resilient infrastructure/ecosystem that ensures the confidentiality, integrity, and availability minimizing the impact of any disruption on mission essential services and functions.,

2. CONTRACT AMOUNT

CDPH has allocated \$800,000 for this contract until funds have been exhausted.

3. CONTRACT TERMS

The estimated term of the Contract shall be September 16, 2021 or upon CDPH approval thru September 15, 2022. Services are based on agreed-to Work Order Authorizations (WOA) for the specific requested services and will continue until allocated funds have been exhausted. The contract will be of no force or effect until it is signed by CDPH. If services commence before final approvals are obtained, said services will be considered voluntary. CDPH reserves the option to terminate this Contract upon completion of services identified herein, exhaustion of funds or upon a ten (10) business day prior written notice if the work is deemed unacceptable.

4. AMENDMENT OF CONTRACT

CDPH reserves the right to amend the Contract when CDPH determines the need to add time for up to one year and/or funds to complete or continue services if the Emergency Proclamation is still in effect. Consideration to amend must be consistent with the terms of the original rates that was agreed upon. Contract amendments are subject to satisfactory performance under the agreement and funding availability.

5. SERVICE LOCATION

The Contractor shall perform the services remotely unless otherwise agreed upon by both parties and based on the project need as proposed in a given Work Order Authorization (WOA).

Contractor and any proposed staff, including subcontractors working onsite will be required to follow the CDPH 21-17-HR Memo, COVID-19 Testing Policy. A copy of the policy will be furnished upon request.

6. SERVICE HOURS

The services shall be provided during normal CDPH working hours of 8:00 a.m. to 5:00 p.m., Monday through Friday, Pacific Time, excluding State of California official holidays. Exceptions may occur if Contractor and the State agree that services are required outside regular working hours for specific activities.

7. PROJECT REPRESENTATIVES

A. The project representatives during the term of this contract will be:

California Department of Public Health Stella Wong, Contract Manager Telephone: (279) 667-0168 E-mail: Stella.Wong@cdph.ca.gov Lisa McCartney, Contract Manager Telephone: (279) 667-0095 E-mail: Lisa.Mccartney@cdph.ca.gov	Deloitte Consulting LLP Christine Huddleson, Contract Manager Telephone: (916) 730-5422 Fax: (415) 783-1149 E-mail: chuddleson@deloitte.com
--	---

B. Direct all inquiries to: 730-5422

California Department of Public Health Attention: Stella Wong/Lisa McCartney 1616 Capitol Avenue, MS 6700 Sacramento, CA 95814 Stella Wong Telephone: (279) 667-0168 E-mail: Stella.Wong@cdph.ca.gov Lisa McCartney Telephone: (279) 667-0095 E-mail: Lisa.Mccartney@cdph.ca.gov	Deloitte Consulting LLP Attention: Christine Huddleson 555 Mission Street San Francisco, CA 94105-0935 Telephone: (916) 730-5422 Fax: (415) 783-1149 E-mail: chuddleson@deloitte.com
---	--

- C. All payments from CDPH to the Contractor; shall be sent to the following address:

Remittance Address
<p>Deloitte Consulting LLP Attention "Cashier": PO Box 844717 980 9th Street, Suite 1800 Sacramento, Ca 95814</p> <p>Telephone: (916) 730-5422 Fax: (415) 783-1149 E-mail: chuddleson@deloitte.com</p>

- D. Either party may make changes to the information above by giving written notice to the other party. Said changes shall not require an amendment to this agreement; however, if the remittance address has changed, the Contractor will be required to submit a completed STD. 204 Payee Data Record form/STD 205 Payee Data Supplement, which must match the invoice address in order to avoid payment delays.

8. QUALIFICATIONS

The contractor and all personnel proposed to perform professional services under the contract must have the mandatory qualifications and experience identified below.

Contractor must provide resumes and references must validate that proposed personnel collectively meet the Contractor knowledge, skills, and experience listed below, including the actual dates of engagement that validate the years of requested skills and experience. Replacement personnel, if needed, must also meet these mandatory qualifications, and authorized by CDPH.

A. Mandatory Qualifications

The Contractor and all proposed personnel must meet the following requirements:

- 1) Demonstrate compliance with meeting auditing standards with respect to State and Federal requirements and with respect to undergoing an external quality control review or at a similar setting.
- 2) Be in good standing and qualified to conduct business in California.
- 3) Demonstrated knowledge and a detailed understanding of large-scale highly complex healthcare, or health related, technical environments and ecosystems.

- 4) Five (5) years of experience analyzing and implementing complex Health Insurance Portability and Accountability Act (HIPAA) based systems and data.
- 5) Five (5) years of experience assessing, implementing, and managing complex systems with implementation cost minimum of or over \$250 million dollars.
- 6) Propose one, or more, personnel. Each personnel must have experience leading three (3) large transformation efforts with a combined cost minimum of or over \$200 million dollars.
- 7) Propose one, or more, personnel. Each personnel must have experience leading 3 large modernization/stabilization efforts with a combined cost of over \$100 million dollars.
- 8) At least one proposed personnel certified in the following related areas:
 - Cloud Computing
 - Security Engineer
 - Solutions/Business Architect.

All proposed personnel must meet the following knowledge, skills, and experience requirements:

- 1) Have a computer science, engineering, mathematics, or technology-related baccalaureate degree from an accredited college or university, or five (5) years of experience in computer science or technology-related field of work.
- 2) Five (5) years of professional work experience in Infrastructure or Enterprise Architecture experienced with:
 - Resolving service or security incidents or emergent technical problems
 - Re-architecting solutions to address impediments
 - Rapidly restoring systems and services after service interruption
- 3) Five (5) years of experience in Systems Integration experienced with:
 - Architecting or re-architecting solutions to optimize solution performance
 - Infrastructure disaster mitigation
 - Infrastructure architecture design in a complex systems environment

B. Desirable Qualifications

The Contractor and all proposed personnel will perform these professional services under the contract:

- 1) Performed similar analyses and assessments for other governmental entities.

- 2) Have demonstrated experience as a technology leader in the modernization and transformation field.

9. SERVICES TO BE PERFORMED

The Contractor is shall provide the following services under this contract:

Task #	TASK DESCRIPTION
Task 1 – Work Plan	
1.1	A brief overview, project plan, and roadmap of the Contractor's approach to the tasks as described in this SOW.
Task 2 – Assessment Report	
2.1	Perform an assessment of the technology ecosystem and end user experience through the underpinning services and technical stack including, but not limited to: Architecture Alignment, System Management, Security, Support (Contractor and/or State Staff), Maintainability, Performance, Scalability, and Availability of the current-state architecture, infrastructure, applications, platforms, cloud environments, and services. The Contractor can take several approached and use all department resources available to them including reviewing documentation, conducting interviews with key staff and subject matter experts (SMEs), and accessing architecture models and process diagrams.
2.2	A written preliminary, and final, assessment report that includes the following: <ol style="list-style-type: none">1) Assessment of the current-state technology ecosystem and horizontal infrastructure view.2) Analysis of the end to infrastructure service and information stack.3) Identification and analysis of core central services.4) Prioritization and classification of mission critical applications.5) Analysis of service support (problem and change management).6) Root cause analysis of major infrastructure and application issues, risks, or vulnerabilities.7) Identification of existing issues, risks, and/or challenges8) Identification of current availability, fault tolerance, and recoverability of the current state.

	<p>9) Initial identification of gaps in the end user experience through the underpinning services and technical stack.</p> <p>10) Identification of processes, support, and system metrics.</p> <p>11) Identification of modernization, stabilization, and/or transformation opportunities.</p> <p>12) Roadmap for defining the appropriate resiliency/stabilization, implementing modernization, improvement opportunities, or mitigating issues, risks, and challenges.</p>
2.3	Prioritize and document critical Information Technology (IT) capabilities, functions, and services that support the organizational goals of CDPH mapping to them components and architectures in the technology ecosystem.
2.4	Evaluate all cloud and network services, infrastructure, environments, and interfaces and recommend cloud optimization improvements to balance performance, availability, resiliency, compliance, and cost against the best-fit infrastructure and architecture.
2.5	Evaluate baseline performance metrics against capacity for critical services in order to determine the level at which service degradation occurs.
2.6	Evaluate and recommend improvement opportunities related to the capabilities of external dependencies (e.g. California Department of Technology, Office of Technology Services (CDT-OTech)) to support the stability of IT services and functions.
2.7	Recommend and prioritize the objectives and recommended improvements for minimizing the risk of failure to critical IT components, applications, middleware, and database systems.
2.8	Evaluate CDPH technology operations and make recommendations on structure, staffing, and processes, including assessing if the appropriate skill and staffing level exists to support the technology and ecosystem.

2.9	Identify, and document use cases associated to root cause analysis associated with end user experience through the underpinning services and technical stack.
2.10	A post-implementation final status report to assess the State of California's progress against provided recommendations.
2.11	Provide final findings & recommendation report with executive summary and supporting details along with a joint presentation to IT Governance Council and/or executive management.
2.12	Assist with the work to remediate findings on as needed basis.

10. CONTRACTOR REPORTING REQUIREMENTS

The Contractor will submit weekly written status reports in MS Word format to the California Department of Public Health Contract Administrator as directed. The reports shall be detailed regarding current status and future activities. Status reports are not considered deliverables under the terms of this Contract. These reports shall include, but not limited to:

- A. A summary of the work completed during the reporting period, showing actual vs. planned.
- B. Highlighted tasks that are behind schedule, adopted remediation plans, and overall impact on the project.
- C. The status of the overall engagement and all phases/projects, including discussion of risks, problems encountered, solutions, and proposed solutions.
- D. The tasks expected to be completed in the next reporting period.
- E. An accounting of Contractor staff person(s) hours for the prior week and for the Contract to date i.e., timesheets.
- F. Ad hoc reporting as required.
- G. If requested, the Contractor shall participate in periodic briefings for Executive Management, as deemed appropriate by the California Department of Public Health.

11. WORK ORDER AUTHORIZATION (WOA)

All Contractor work will be authorized in advance by the State via a signed WOA. WOAs will authorize services that are within the scope of this contract. It is

understood and agreed by both parties to this Contract that all terms and conditions of this Contract shall remain in force. Such WOA shall in no way constitute a Contract other than as provided pursuant to this Contract nor in any way amend or supersede any of the other provisions of this final Contract.

Under no circumstance shall the Contractor be entitled for payment for preparatory expenses and any anticipated future needs. Personnel resources expended on task accomplishment in excess of the cost authorized in the WOA will be at no cost to the State. All WOAs will be reviewed during Planning sessions and must signed by the CDPH Contract Manager, CDPH Program Designee and other identified CDPH staff and Contractor prior to beginning work. Once the work is complete, the CDPH Contractor Manager will approve the WOA for payment. The goal for the WOA is to ensure that the CDPH and Contractor have a common understanding of the scope, schedule, format, and content of work to be performed prior to beginning work.

A. WOA Procedures

A sample WOA form is included as Attachment 2C.

B. WOA Approval

All work or work products related to WOAs shall be subject to the State's Acceptance, along with all supporting work product materials and documents, including working papers, test scripts, test results, reference materials, etc. All supporting working materials and documents are the property of the State and shall be available to the State upon request. It is at the State's sole determination as to whether work or work products related to a WOA are acceptable. No work shall be accepted by the State for review without a WOA.

Before an invoice can be created and submitted to CDPH for payment, the CDPH Designee must sign off on the related WOA as being complete and acceptable. It shall be CDPH's sole determination as to whether a WOA has been successfully completed and is acceptable to the CDPH.

12. CONTRACTOR ADMINISTRATIVE REQUIREMENTS

A. Contractor Contract Manager

The Contractor shall designate a Contract Manager (CM) to whom all project communications may be addressed and has the authority to act on all aspects of the project, as well as the contact for all Contractor staffing and invoicing issues. The Contractor's personnel shall work as part of an integrated team of professionals to deliver quality services in a timely manner. Effective teamwork is essential to the successfully completion of the required tasks. Contractor personnel should continue to keep their knowledge and skills up to date throughout the term of the Contract.

B. Contractor Personnel Changes

The Contractor is required to maintain staff continuity throughout the life of the project. CDPH will be notified in writing of any changes 10 days prior to the personnel assigned to tasks. If a Contractor's employee is unable to perform his or her duties due to illness, resignation, emotional instability, incarceration, or other factors that is beyond the Contractor's control, the Contractor will make every reasonable effort to provide suitable substitute personnel. Prior to initiating work, the substitute personnel must meet all requirements of this SOW, provide a resume and sample work, and must be approved in writing by CDPH.

C. Qualified Staff and Resumes

The Contractor is responsible for ensuring the proposed staff, including subcontractors provided meets the qualifications, certifications and experience required to perform the work identified for the project role/classification they are fulfilling. The Contractor must provide to the CDPH contract manager or designee, a resume, and any required documentation by CDPH for each proposed staff for CDPH review and approval as described in Section 8 above. CDPH approval must be obtained in writing prior to the proposed staff beginning work.

D. Equipment and Software

The Contractor will provide its own equipment and software necessary to perform the required duties.

E. Submission of Invoices

- 1) Payment for services performed under the Procurement shall be made in accordance with the State of California's Prompt Payment Act (GC Section 927 et seq.).

Invoices shall be submitted in arrears after the WOA work is concluded and CDPH notifies the Contractor that work is accepted. The Contractor shall submit invoices to the CDPH Contract Manager identifying staff classification, associated hours, labor rates and total amount invoiced as agreed upon in Attachment 2A – Cost Worksheet. No more than one invoice can be processed during a monthly period. A sample invoice format is included in Attachment 2B.

- 2) Invoice submissions must include the following:

- 1) Signed Invoice
- 2) Contractors' timesheets
- 3) Approved WOA associated with the invoice submittal

F. Problem Escalation

The Contractor may wish to escalate issues. Such issues may include, but are not necessarily limited to, invoice processing and CDPH timeliness in meeting its other contractual obligations. There may be instances where the severity of the problem justifies escalated reporting. To this extent, the Contractor will determine the level of severity and notify the appropriate CDPH personnel as specified below.

The Contractor shall advise the CDPH Contract Manager of any intended escalation. If the Contractor is not satisfied that CDPH is exercising its best efforts to resolve any problem or issue in an appropriate amount of time, the Contractor may escalate the problem or issue to the next appropriate level(s).

CDPH personnel are to be notified in the following sequence:

1. First level: CDPH Contract Manager
2. Second level: CDPH Chief Technology Officer

G. Artifact Format

Unless explicitly stated otherwise, all Artifacts shall be provided in Microsoft Word 2016 Microsoft Excel 2016, Microsoft PowerPoint 2016, Visio 2013 or Microsoft Project 2010. This applies, but is not limited to, word processing documents, spreadsheets, schedules, and presentations. Artifacts must be well organized, free of spelling or typographical errors, grammatically correct and contain pertinent, up to date information when submitted to CDPH.

H. ADA Compliance

Contractor shall ensure that all work under this contract meets and comply with the ADA standards.

I. Return of State Property

Return all state property, including state badges upon termination or completion of the contract.

13. STATE RESPONSIBILITIES

CDPH shall provide the following:

- A. Designate a CM who will coordinate WOA completion and all communications with the Contractor. The CM has the authority to act on all aspects of the service. The person will review the SOW and associated documents with the Contractor to ensure understand of the responsibilities of both parties.
- B. The required software and hardware.

- C. Work with the Contractor to provide clarifications of the services, as outlined above, WOA process, and associated expectations.
- D. Access to appropriate levels of staff, stakeholders, users, and department management for successful completion of project activities.
- E. Approve any staffing changes in advance and must meet all qualification as identified in Section 8 above.
- F. Promote timely decisions and reviews of WOAs and Work Products.
- G. Pay invoices based on CDPH acceptance of approved Work Products and upon approval of the WOA.
- H. Review invoices and associated documents within ten (10) business days of receipt and notify the Contractor in writing of acceptance or dispute.
- I. Building access and workspace for Contractor staff, as needed to work onsite as mutually agreed upon.
- J. It shall be CDPH's sole determination as to whether a task has been successfully completed.

11. SUBCONTRACTOR

Subcontractors may be utilized for this contract and must meet required qualifications in Section 8 above.

ATTACHMENT 2
Agency Special Provisions

1. Invoicing and Payment

- A. In no event shall the Contractor request reimbursement from the State for obligations entered into or for costs incurred prior to the commencement date or after the expiration of this Agreement.
- B. For services satisfactorily rendered, and upon receipt and final approval of the invoices, the State agrees to compensate the Contractor for actual services performed and accepted in accordance with the Project Role/Classification rates specified in Attachment 2A – Cost Worksheet.
- C. Invoices shall be submitted monthly, in arrears, no later than 30 days after the end of the billing period.

Invoices must be submitted electronically via email to Wilson Yee at CDPH_ITSDinv@cdph.ca.gov and include Agreement Number 21-10459 on the subject line. A sample invoice format is included in Attachment 2B.

The State, at its discretion, may designate an alternate invoice submission email address. A change in invoice address shall be accomplished via a written notice to the Contractor by State and shall not require an amendment to this agreement.

- 1) Invoices shall be accompanied by a Work Order Authorization (WOA), as identified in Attachment 1 – SOW and contain the following:
 - 1) Be prepared on Contractor letterhead.
 - 2) Invoices must be submitted to CDPH electronically.
 - 3) Identify the billing and/or performance period covered by the invoice.
 - 4) Itemize costs (labor category hours with hourly rates) for the billing period in the same or greater level of detail as indicated in this agreement. Subject to the terms of this agreement, reimbursement may only be sought for those costs and/or cost categories expressly identified as allowable in this agreement and approved by the CDPH.
 - 5) Provide supporting documentation as required in this Agreement.

2) Amounts Payable

The amounts payable under this agreement shall not exceed \$800,000 for the term of this agreement.

3) Rates Payable

Contractor will be reimbursed for services satisfactory performed based on the rate schedule identified in Attachment 2A – Cost Worksheet.

2. Budget Contingency Clause

- A. It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Agreement does not appropriate sufficient funds for the program, this Agreement shall be of no further force and effect. In this event, the State shall have no

liability to pay any funds whatsoever to Contractor or to furnish any other considerations under this Agreement and Contractor shall not be obligated to perform any provisions of this Agreement.

- B. If funding for any fiscal year is reduced or deleted by the Budget Act for purposes of this program, the State shall have the option to either cancel this Agreement with no liability occurring to the State, or offer an agreement amendment to Contractor to reflect the reduced amount.

3. Prompt Payment Clause

Payment will be made in accordance with, and within the time specified in, Government Code Chapter 4.5, commencing with Section 927.

4. Timely Submission of Final Invoice

- A. A final undisputed invoice shall be submitted for payment no more than thirty (60) calendar days following the expiration or termination date of this agreement, unless a later or alternate deadline is agreed to in writing by the program contract manager. Said invoice should clearly mark "Final Invoice", indicating that all payment obligations of the State under this agreement have ceased and that no further payments are due or outstanding. The State may, at its discretion, choose not to honor any delinquent final invoice if the Contractor fails to obtain prior written State approval of an alternate final invoice submission deadline.
- B. The Contractor is hereby advised of its obligation to submit to the state, with the final invoice, a completed copy of the "Contractor's Release (Attachment 4)".

5. Expense Allowability/Fiscal Documentation

- A. Invoices, received from the Contractor and accepted for payment by the State, shall not be deemed evidence of allowable agreement costs.
- B. Contractor shall maintain for review and audit and supply to CDPH upon request, adequate documentation of all expenses claimed pursuant to this agreement to permit a determination of expense allowability.
- C. If the allowability of an expense cannot be determined by the State because invoice detail, fiscal records, or backup documentation is nonexistent or inadequate according to generally accepted accounting principles or practices, all questionable costs may be disallowed and payment may be withheld by the State. Upon receipt of adequate documentation supporting a disallowed or questionable expense, reimbursement may resume for the amount substantiated and deemed allowable.

6. Recovery of Overpayments

- A. Contractor agrees that claims based upon the terms of this agreement or an audit finding and/or an audit finding that is appealed and upheld, will be recovered by the State by one of the following options:
- 1) Contractor's remittance to the State of the full amount of the audit exception within 30 days following the State's request for repayment.

- 2) A repayment schedule agreeable between the State and the Contractor.
- B. The State reserves the right to select which option as indicated above in paragraph A will be employed and the Contractor will be notified by the State in writing of the claim procedure to be utilized.
- C. Interest on the unpaid balance of the audit finding or debt will accrue at a rate equal to the monthly average of the rate received on investments in the Polled Money Investment Fund commencing on the date that an audit or examination finding is mailed to the Contractor, beginning 30 days after the Contractor's receipt of the State's demand for repayment.
- D. If the Contractor has filed a valid appeal regarding the report of audit finding recovery of the overpayments will be deferred until a final administrative decision on the appeal has been reached. If the Contractor loses the final administrative appeal, Contractor shall repay, to the State, the over-claimed or disallowed expenses, plus accrued interest. Interest accrues from the Contractor's first receipt of State's notice requesting reimbursement of questioned audit costs or disallowed expenses.

7. Travel and Per Diem Reimbursement

The State will not be reimbursing for any travel under this agreement.

ATTACHMENT 2A
COST WORKSHEET

- List the Name, Project Role/Classification, and hourly rate of the proposed staff, including subcontractors.
- Provide a resume for each proposed staff listed.

Name	Project Role/Classification	Sub-contractor (yes/no)	Hourly Rate
Aswin Kathirasetty	Senior Enterprise Architect	No	\$ 200/hour*
Lenin Vyas	Senior Technical Lead	No	\$ 190/hour*
William Campos	Info Security Specialist	No	\$ 190/hour
TBD	Enterprise Architect	TBD	\$ 180/hour*
TBD	Technical Lead	TBD	\$ 175/hour
TBD	Senior Programmer	TBD	\$ 135/hour
TBD	Programmer	TBD	\$ 119/hour

* Our proposed hourly rates for Senior Enterprise Architect, Senior Technical Lead and Enterprise Architect have been discounted from our negotiated IT MSA Rates.

1. CDPH has allocated \$800,000 for this contract.
2. Payments will be based on the completion and acceptance of the specific WOAs. The Contractor is only entitled to reimbursement for time and materials directly related to properly issued work orders, and in no circumstance shall the Contractor be entitled to payment for preparatory expenses for anticipated future needs. Personnel resources expended on task accomplishment in excess of the cost authorized in the WOA will be at no cost to the State.
3. The Offeror further understands that the hourly rates must be fully loaded, including but not limited to, operating expenses, labor, transportation/travel costs, per diem expenses, equipment costs, supplies, overhead, annual inflation costs/rate adjustments, profit margin, taxes, shipping, and etc.
4. No travel will be reimbursed under this contract.
5. Subcontractors may be utilized for this project with prior approval from CDPH.

The Contractor hereby certifies that the hourly rate(s) submitted on this Cost Worksheet are true and accurate to the best of its knowledge and shall remain in effect throughout the term. Amendment, if allowed, must be consistent with original rates agreed upon on this Cost Worksheet.

**ATTACHMENT 2B
INVOICE FORMAT (SAMPLE)**

(Company letterhead must be included)

Date Submitted:

California Department of Public Health

Attn: CDPH Contract Manager

Name:

Address:

Phone Number:

Invoice No.:

Contract No.:

FI\$Cal Purchase Order No.:

Small Business/Disable Veteran Business Enterprise (DVBE) (if applicable):

This invoice requests payment of the following Work Order Authorizations (WOAs):

WOA #	WOA Description	Hours	Amount
Total:			

Remit Payment to:

Contractor's Legal Business Name

Remittance Address

City, State, Zip

Attn: Authorized Representative Name

Title:

Phone Number:

Comments:

Authorized Representative Signature

Note: Contractor's remittance information above must match the Payee Data Record (STD 204) for each invoice submitted. A new STD 204 must be submitted to change address information. Do not include the Taxpayer Identification Number (TIN).

CDPH USE ONLY

I certify that the above have been received and accepted as complete:

CDPH/ITSD Manager

Date

Phone

ATTACHMENT 2C
WORK ORDER AUTHORIZATION (SAMPLE)

CDPH USE ONLY									
Contract #:				WOA #:					
Fiscal Year:			Start Date:			End Date:			
Approp Ref	Fund	Account	Alt Account	Program	Project ID	Activity ID	Reporting Structure	Service Location	Actual Cost ^①
									\$
*TOTAL ACTUAL COST:									\$

^①Actual Cost will be entered upon work completion and invoice hours/costs validation.

*Total actual cost must match the invoice. Total cost on the invoice cannot exceed total estimated cost on WOA (unless otherwise agreed upon by both parties) and must align with the timesheets.

SECTION 1: Work Order Authorization and Approval to Begin Work

The **Work Order Authorization** Section describes the planned work products associated to this WOA and lists Contractors hours to complete the work. Work Products will be identified during the planning session and accepted during the review sessions. The signatures below authorize work to begin:

[CM Completes This Section]

WOA #	WOA Title#:
Start Date: XX/XX/XXXX	Completion Date: XX/XX/XXXX
Work Description:	

Total Contractor hours required for WOA.

This section provides the Estimated Hours/Costs associated with individuals required for this WOA. The signatures below authorize work to begin.

[Contractor Completes This Section]

#	Classification	Name	Labor Rate*	Estimated Hours	Cost Estimate
1					\$
2					\$
3					\$
4					\$
5					\$
6					\$
Total Estimated Hours / Cost:					\$

*Labor rates must not exceed the approved MSA classifications and hourly labor rates as agreed upon in the agreement.

[CM Obtain Signatures To Authorize Work To Begin]

Organization / Role	Name	Signature	Date
Contractor Contract Manager			
CA Department of Public Health Program Designee			
CA Department of Public Health Contract Manager			

SECTION 2: Work Order Approval to Invoice

The **Work Order Approval to Invoice** insures the following:

- Invoiced hourly rate aligns with contract.
- Invoiced costs do not exceed **Total Estimated Costs** for this WOA, unless otherwise agreed upon by both parties.
- Staff timesheets provided match actual days and hours worked.

SECTION 3: Work Order Approval and Payment

The **Work Order Approval and Payment** Section contain signature approving work completion and for the Contractor to submit an invoice for payment.

CDPH agrees to pay for the Work Products as described in this WOA. Work Products **NOT** completed are listed above showing final disposition (e.g. Product Backlog).

APPROVAL TO INVOICE FOR PAYMENT

The signature below approves the payment of the WOA. The Contractor is responsible for Invoicing CDPH as outlined in the agreement number referenced above.

[CM To Obtain Final Signature]

Organization / Role	Name	Signature	Date
CA Department of Public Health Contract Manager			

Note: Invoices must include Contractor timesheets and cannot exceed "Total Estimated Cost" listed on page 1 of this WOA, unless otherwise agreed upon by both parties.

ATTACHMENT 3
INFORMATION TECHNOLOGY GENERAL PROVISIONS

1. **DEFINITIONS:** Unless otherwise specified in the Statement of Work, the following terms shall be given the meaning shown, unless context requires otherwise.
- a) "**Acceptance Tests**" means those tests performed during the Performance Period which are intended to determine compliance of Equipment and Software with the specifications and all other Attachments incorporated herein by reference and to determine the reliability of the Equipment.
 - b) "**Application Program**" means a computer program which is intended to be executed for the purpose of performing useful work for the user of the information being processed. Application programs are developed or otherwise acquired by the user of the Hardware/Software system, but they may be supplied by the Contractor.
 - c) "**Attachment**" means a mechanical, electrical, or electronic interconnection to the Contractor-supplied Machine or System of Equipment, manufactured by other than the original Equipment manufacturer that is not connected by the Contractor.
 - d) "**Business entity**" means any individual, business, partnership, joint venture, corporation, S-corporation, limited liability company, sole proprietorship, joint stock company, consortium, or other private legal entity recognized by statute.
 - e) "**Buyer**" means the State's authorized contracting official.
 - f) "**Commercial Hardware**" means Hardware developed or regularly used that: (i) has been sold, leased, or licensed to the general public; (ii) has been offered for sale, lease, or license to the general public; (iii) has not been offered, sold, leased, or licensed to the public but will be available for commercial sale, lease, or license in time to satisfy the delivery requirements of this Contract; or (iv) satisfies a criterion expressed in (i), (ii), or (iii) above and would require only minor modifications to meet the requirements of this Contract.
 - g) "**Commercial Software**" means Software developed or regularly used that: (i) has been sold, leased, or licensed to the general public; (ii) has been offered for sale, lease, or license to the general public; (iii) has not been offered, sold, leased, or licensed to the public but will be available for commercial sale, lease, or license in time to satisfy the delivery requirements of this Contract; or (iv) satisfies a criterion expressed in (i), (ii), or (iii) above and would require only minor modifications to meet the requirements of this Contract.
 - h) "**Contract**" means this Contract or agreement (including any purchase order), by whatever name known or in whatever format used.
 - i) "**Custom Software**" means Software that does not meet the definition of Commercial Software.
 - j) "**Contractor**" means the Business Entity with whom the State enters into this Contract. Contractor shall be synonymous with "supplier", "vendor" or other similar term.
 - k) "**Data Processing Subsystem**" means a complement of Contractor-furnished individual Machines, including the necessary controlling elements (or the functional equivalent), Operating Software and Software, if any, which are acquired to operate as an integrated group, and which are interconnected entirely by Contractor-supplied power and/or signal cables; e.g., direct access controller and drives, a cluster of terminals with their controller, etc.
 - l) "**Data Processing System (System)**" means the total complement of Contractor-furnished Machines, including one or more central processors (or instruction processors), Operating Software which are acquired to operate as an integrated group.
 - m) "**Deliverables**" means Goods, Software, Information Technology, telecommunications technology, Hardware, and other items (e.g. reports) to be delivered pursuant to this Contract, including any such items furnished incident to the provision of services.
 - n) "**Designated CPU(s)**" means for each product, if applicable, the central processing unit of the computers or the server unit, including any associated peripheral units. If no specific "Designated CPU(s)" are specified on the Contract, the term shall mean any and all CPUs located at the site specified therein.
 - o) "**Documentation**" means manuals and other printed materials necessary or useful to the State in its use or maintenance of the Equipment or Software provided hereunder. Manuals and other printed materials customized for the State hereunder constitute Work Product if such materials are required by the Statement of Work.
 - p) "**Equipment**" is an all-inclusive term which refers either to individual Machines or to a complete Data Processing System or Subsystem, including its Hardware and Operating Software (if any).
 - q) "**Equipment Failure**" is a malfunction in the Equipment, excluding all external factors, which prevents the accomplishment of the Equipment's intended function(s). If microcode or Operating Software residing in the Equipment is necessary for the proper operation of the Equipment, a failure of such microcode or Operating Software which prevents the accomplishment of the Equipment's intended functions shall be deemed to be an Equipment Failure.
 - r) "**Facility Readiness Date**" means the date specified in the Statement of Work by which the State must have the site prepared and available for Equipment delivery and installation.
 - s) "**Goods**" means all types of tangible personal property, including but not limited to materials, supplies, and Equipment (including computer and telecommunications Equipment).
 - t) "**Hardware**" usually refers to computer Equipment and is contrasted with Software. See also Equipment.
 - u) "**Installation Date**" means the date specified in the Statement of Work by which the Contractor must have the ordered Equipment ready (certified) for use by the State.
 - v) "**Information Technology**" includes, but is not limited to, all electronic technology systems and services, automated information handling, System design and analysis, conversion of data, computer programming, information storage and retrieval, telecommunications which include voice, video, and data communications, requisite System controls, simulation, electronic commerce, and all related interactions between people and Machines.
 - w) "**Machine**" means an individual unit of a Data Processing System or Subsystem, separately identified by a type and/or model number, comprised of but not limited to mechanical, electro-mechanical, and electronic parts, microcode, and special features installed thereon and including any necessary Software, e.g., central processing unit, memory module, tape unit, card reader, etc.
 - x) "**Machine Alteration**" means any change to a Contractor-supplied Machine which is not made by the Contractor, and which results in the Machine deviating from its physical, mechanical, electrical, or electronic (including microcode) design, whether or not additional devices or parts are employed in making such change.
 - y) "**Maintenance Diagnostic Routines**" means the diagnostic programs customarily used by the Contractor to test Equipment for proper functioning and reliability.
 - z) "**Manufacturing Materials**" means parts, tools, dies, jigs, fixtures, plans, drawings, and information produced or acquired, or rights acquired, specifically to fulfill obligations set forth herein.
 - aa) "**Mean Time Between Failure (MTBF)**" means the average expected or observed time between consecutive failures in a System or component.
 - bb) "**Mean Time to Repair (MTTR)**" means the average expected or observed time required to repair a System or component and return it to normal operation.

- cc) "**Operating Software**" means those routines, whether or not identified as Program Products, that reside in the Equipment and are required for the Equipment to perform its intended function(s), and which interface the operator, other Contractor-supplied programs, and user programs to the Equipment.
 - dd) "**Operational Use Time**" means for performance measurement purposes, that time during which Equipment is in actual operation by the State. For maintenance Operational Use Time purposes, that time during which Equipment is in actual operation and is not synonymous with power on time.
 - ee) "**Period of Maintenance Coverage**" means the period of time, as selected by the State, during which maintenance services are provided by the Contractor for a fixed monthly charge, as opposed to an hourly charge for services rendered. The Period of Maintenance Coverage consists of the Principal Period of Maintenance and any additional hours of coverage per day, and/or increased coverage for weekends and holidays.
 - ff) "**Preventive Maintenance**" means that maintenance, performed on a scheduled basis by the Contractor, which is designed to keep the Equipment in proper operating condition.
 - gg) "**Principal Period of Maintenance**" means any nine consecutive hours per day (usually between the hours of 7:00 a.m. and 6:00 p.m.) as selected by the State, including an official meal period not to exceed one hour, Monday through Friday, excluding holidays observed at the installation.
 - hh) "**Programming Aids**" means Contractor-supplied programs and routines executable on the Contractor's Equipment which assists a programmer in the development of applications including language processors, sorts, communications modules, data base management systems, and utility routines, (tape-to-disk routines, disk-to-print routines, etc.).
 - ii) "**Program Product**" means programs, routines, subroutines, and related items which are proprietary to the Contractor and which are licensed to the State for its use, usually on the basis of separately stated charges and appropriate contractual provisions.
 - jj) "**Remedial Maintenance**" means that maintenance performed by the Contractor which results from Equipment (including Operating Software) failure, and which is performed as required, i.e., on an unscheduled basis.
 - kk) "**Software**" means an all-inclusive term which refers to any computer programs, routines, or subroutines supplied by the Contractor, including Operating Software, Programming Aids, Application Programs, and Program Products.
 - ll) "**Software Failure**" means a malfunction in the Contractor-supplied Software, other than Operating Software, which prevents the accomplishment of work, even though the Equipment (including its Operating Software) may still be capable of operating properly. For Operating Software failure, see definition of Equipment Failure.
 - mm) "**State**" means the government of the State of California, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the State of California.
 - nn) "**System**" means the complete collection of Hardware, Software and services as described in this Contract, integrated and functioning together, and performing in accordance with this Contract.
 - oo) "**U.S. Intellectual Property Rights**" means intellectual property rights enforceable in the United States of America, including without limitation rights in trade secrets, copyrights, and U.S. patents.
- 2. CONTRACT FORMATION:**
- a) If this Contract results from a sealed bid offered in response to a solicitation conducted pursuant to Chapters 2 (commencing with Section 10290), 3 (commencing with
- Section 12100), and 3.6 (commencing with Section 12125) of Part 2 of Division 2 of the Public Contract Code (PCC), then Contractor's bid is a firm offer to the State which is accepted by the issuance of this Contract and no further action is required by either party.
- b) If this Contract results from a solicitation other than described in paragraph a), above, the Contractor's quotation or proposal is deemed a firm offer and this Contract document is the State's acceptance of that offer.
 - c) If this Contract resulted from a joint bid, it shall be deemed one indivisible Contract. Each such joint Contractor will be jointly and severally liable for the performance of the entire Contract. The State assumes no responsibility or obligation for the division of orders or purchases among joint Contractors.
- 3. COMPLETE INTEGRATION:** This Contract, including any documents incorporated herein by express reference, is intended to be a complete integration and there are no prior or contemporaneous different or additional agreements pertaining to the subject matter of the Contract.
- 4. SEVERABILITY:** The Contractor and the State agree that if any provision of this Contract is found to be illegal or unenforceable, such term or provision shall be deemed stricken and the remainder of the Contract shall remain in full force and effect. Either party having knowledge of such term or provision shall promptly inform the other of the presumed non-applicability of such provision.
- 5. INDEPENDENT CONTRACTOR:** Contractor and the agents and employees of the Contractor, in the performance of this Contract, shall act in an independent capacity and not as officers or employees or agents of the State.
- 6. APPLICABLE LAW:** This Contract shall be governed by and shall be interpreted in accordance with the laws of the State of California; venue of any action brought with regard to this Contract shall be in Sacramento County, Sacramento, California. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Contract.
- 7. COMPLIANCE WITH STATUTES AND REGULATIONS:**
- a) The State and the Contractor warrants and certifies that in the performance of this Contract, it will comply with all applicable statutes, rules, regulations and orders of the United States and the State of California. The Contractor agrees to indemnify the State against any loss, cost, damage or liability by reason of the Contractor's violation of this provision.
 - b) The State will notify the Contractor of any such claim in writing and tender the defense thereof within a reasonable time; and
 - c) The Contractor will have sole control of the defense of any action on such claim and all negotiations for its settlement or compromise; provided that (i) when substantial principles of government or public law are involved, when litigation might create precedent affecting future State operations or liability, or when involvement of the State is otherwise mandated by law, the State may participate in such action at its own expense with respect to attorneys' fees and costs (but not liability); (ii) where a settlement would impose liability on the State, affect principles of California government or public law, or impact the authority of the State, the Department of General Services will have the right to approve or disapprove any settlement or compromise, which approval will not unreasonably be withheld or delayed; and (iii) the State will reasonably cooperate in the defense and in any related settlement negotiations.
 - d) If this Contract is in excess of \$554,000, it is subject to the requirements of the World Trade Organization (WTO) Government Procurement Agreement (GPA).
 - e) To the extent that this Contract falls within the scope of Government Code Section 11135, the Contractor hereby agrees to respond to and resolve any complaint brought to

- its attention, regarding accessibility of its products or services.
- 8. CONTRACTOR'S POWER AND AUTHORITY:** The Contractor warrants that it has full power and authority to grant the rights herein granted and will hold the State harmless from and against any loss, cost, liability, and expense (including reasonable attorney fees) arising out of any breach of this warranty. Further, the Contractor avers that it will not enter into any arrangement with any third party which might abridge any rights of the State under this Contract.
- The State will notify the Contractor of any such claim in writing and tender the defense thereof within a reasonable time; and
 - The Contractor will have sole control of the defense of any action on such claim and all negotiations for its settlement or compromise; provided that (i) when substantial principles of government or public law are involved, when litigation might create precedent affecting future State operations or liability, or when involvement of the State is otherwise mandated by law, the State may participate in such action at its own expense with respect to attorneys' fees and costs (but not liability); (ii) where a settlement would impose liability on the State, affect principles of California government or public law, or impact the authority of the State, the Department of General Services will have the right to approve or disapprove any settlement or compromise, which approval will not unreasonably be withheld or delayed; and (iii) the State will reasonably cooperate in the defense and in any related settlement negotiations.
- 9. ASSIGNMENT:** This Contract shall not be assignable by the Contractor in whole or in part without the written consent of the State. The State's consent shall not be unreasonably withheld or delayed. For the purpose of this paragraph, the State will not unreasonably prohibit the Contractor from freely assigning its right to payment, provided that the Contractor remains responsible for its obligations hereunder.
- 10. WAIVER OF RIGHTS:** Any action or inaction by the State or the failure of the State on any occasion, to enforce any right or provision of the Contract, shall not be construed to be a waiver by the State of its rights hereunder and shall not prevent the State from enforcing such provision or right on any future occasion. The rights and remedies of the State herein are cumulative and are in addition to any other rights or remedies that the State may have at law or in equity.
- 11. ORDER OF PRECEDENCE:** In the event of any inconsistency between the articles, attachments, specifications or provisions which constitute this Contract, the following order of precedence shall apply:
- These General Provisions – Information Technology (In the instances provided herein where the paragraph begins: "Unless otherwise specified in the Statement of Work" provisions specified in the Statement of Work replacing these paragraphs shall take precedence over the paragraph referenced in these General Provisions);
 - Contract form, i.e., Purchase Order STD 65, Standard Agreement STD 213, etc., and any amendments thereto;
 - Other Special Provisions;
 - Statement of Work, including any specifications incorporated by reference herein;
 - Cost worksheets; and
 - All other attachments incorporated in the Contract by reference.
- 12. PACKING AND SHIPMENT:**
- All Goods are to be packed in suitable containers for protection in shipment and storage, and in accordance with applicable specifications. Each container of a multiple container shipment shall be identified to:
 - show the number of the container and the total number of containers in the shipment; and
 - the number of the container in which the packing sheet has been enclosed.

(REVISED AND EFFECTIVE 9/5/14)

- All shipments by the Contractor or its subcontractors must include packing sheets identifying: the State's Contract number; item number; quantity and unit of measure; part number and description of the Goods shipped; and appropriate evidence of inspection, if required. Goods for different Contracts shall be listed on separate packing sheets.
 - Shipments must be made as specified in this Contract, as it may be amended, or otherwise directed in writing by the State's Transportation Management Unit within the Department of General Services, Procurement Division.
- 13. TRANSPORTATION COSTS AND OTHER FEES OR EXPENSES:** No charge for delivery, drayage, express, parcel post, packing, cartage, insurance, license fees, permits, cost of bonds, or for any other purpose will be paid by the State unless expressly included and itemized in the Contract.
- The Contractor must strictly follow Contract requirements regarding Free on Board (F.O.B.), freight terms and routing instructions. The State may permit use of an alternate carrier at no additional cost to the State with advance written authorization of the Buyer.
 - If "prepay and add" is selected, supporting freight bills are required when over \$50, unless an exact freight charge is approved by the Transportation Management Unit within the Department of General Services Procurement Division and a waiver is granted.
 - On "F.O.B. Shipping Point" transactions, should any shipments under the Contract be received by the State in a damaged condition and any related freight loss and damage claims filed against the carrier or carriers be wholly or partially declined by the carrier or carriers with the inference that damage was the result of the act of the shipper such as inadequate packaging or loading or some inherent defect in the Equipment and/or material, the Contractor, on request of the State, shall at Contractor's own expense assist the State in establishing carrier liability by supplying evidence that the Equipment and/or material was properly constructed, manufactured, packaged, and secured to withstand normal transportation conditions.
- 14. DELIVERY:** The Contractor shall strictly adhere to the delivery and completion schedules specified in this Contract. Time, if stated as a number of days, shall mean calendar days unless otherwise specified. The quantities specified herein are the only quantities required. If the Contractor delivers in excess of the quantities specified herein, the State shall not be required to make any payment for the excess Deliverables, and may return them to Contractor at the Contractor's expense or utilize any other rights available to the State at law or in equity.
- 15. SUBSTITUTIONS:** Substitution of Deliverables may not be tendered without advance written consent of the Buyer. The Contractor shall not use any specification in lieu of those contained in the Contract without written consent of the Buyer.
- 16. INSPECTION, ACCEPTANCE AND REJECTION:** Unless otherwise specified in the Statement of Work:
- When acquiring Commercial Hardware or Commercial Software, the State shall rely on Contractor's existing quality assurance system as a substitute for State inspection and testing. For all other acquisitions, Contractor and its subcontractors will provide and maintain a quality assurance system acceptable to the State covering Deliverables and services under this Contract and will tender to the State only those Deliverables that have been inspected and found to conform to this Contract's requirements. The Contractor will keep records evidencing inspections and their result, and will make these records available to the State during Contract performance and for three years after final payment. The Contractor shall permit the State to review procedures, practices, processes, and related documents to determine the acceptability of the Contractor's quality assurance System or other similar business practices related to performance of the Contract.

- b) All Deliverables may be subject to inspection and test by the State or its authorized representatives.
- c) The Contractor and its subcontractors shall provide all reasonable facilities for the safety and convenience of inspectors at no additional cost to the State. The Contractor shall furnish to inspectors all information and data as may be reasonably required to perform their inspection.
- d) Subject to subsection 16 (a) above, all Deliverables may be subject to final inspection, test and acceptance by the State at destination, notwithstanding any payment or inspection at source..
- e) The State shall give written notice of rejection of Deliverables delivered or services performed hereunder within a reasonable time after receipt of such Deliverables or performance of such services. Such notice of rejection will state the respects in which the Deliverables do not substantially conform to their specifications. If the State does not provide such notice of rejection within fifteen (15) days of delivery for purchases of Commercial Hardware or Commercial Software or thirty (30) days of delivery for all other purchases, such Deliverables and services will be deemed to have been accepted. Acceptance by the State will be final and irreversible, except as it relates to latent defects, fraud, and gross mistakes amounting to fraud. Acceptance shall not be construed to waive any warranty rights that the State might have at law or by express reservation in this Contract with respect to any nonconformity.
- f) Unless otherwise specified in the Statement of Work, title to Equipment shall remain with the Contractor and assigns, if any, until such time as successful acceptance testing has been achieved. Title to a special feature installed on a Machine and for which only a single installation charge was paid shall pass to the State at no additional charge, together with title to the Machine on which it was installed.

17. SAMPLES:

- a) Samples of items may be required by the State for inspection and specification testing and must be furnished free of expense to the State. The samples furnished must be identical in all respects to the products bid and/or specified in the Contract.
- b) Samples, if not destroyed by tests, may, upon request made at the time the sample is furnished, be returned at the Contractor's expense.

18. WARRANTY:

- a) Unless otherwise specified in the Statement of Work, the warranties in this subsection a) begin upon delivery of the goods or services in question and end one (1) year thereafter. The Contractor warrants that (i) Deliverables and services furnished hereunder will substantially conform to the requirements of this Contract (including without limitation all descriptions, specifications, and drawings identified in the Statement of Work), and (ii) the Deliverables will be free from material defects in materials and workmanship. Where the parties have agreed to design specifications (such as a Detailed Design Document) and incorporated the same or equivalent in the Statement of Work directly or by reference, the Contractor will warrant that its Deliverables provide all material functionality required thereby. In addition to the other warranties set forth herein, where the Contract calls for delivery of Commercial Software, the Contractor warrants that such Software will perform in accordance with its license and accompanying Documentation. The State's approval of designs or specifications furnished by Contractor shall not relieve the Contractor of its obligations under this warranty.
- b) The Contractor warrants that Deliverables furnished hereunder (i) will be free, at the time of delivery, of harmful code (i.e. computer viruses, worms, trap doors, time bombs, disabling code, or any similar malicious mechanism designed to interfere with the intended operation of, or cause damage to, computers, data, or Software); and (ii) will not infringe or violate any U.S. Intellectual Property Right.

Without limiting the generality of the foregoing, if the State believes that harmful code may be present in any Commercial Software delivered hereunder, the Contractor will, upon the State's request, provide a new or clean install of the Software.

- c) Unless otherwise specified in the Statement of Work:
 - (i) The Contractor does not warrant that any Software provided hereunder is error-free or that it will run without immaterial interruption.
 - (ii) The Contractor does not warrant and will have no responsibility for a claim to the extent that it arises directly from (A) a modification made by the State, unless such modification is approved or directed by the Contractor, (B) use of Software in combination with or on products other than as specified by the Contractor, or (C) misuse by the State.
 - (iii) Where the Contractor resells Commercial Hardware or Commercial Software it purchased from a third party, Contractor, to the extent it is legally able to do so, will pass through any such third party warranties to the State and will reasonably cooperate in enforcing them. Such warranty pass-through will not relieve the Contractor from Contractor's warranty obligations set forth above.
- d) All warranties, including special warranties specified elsewhere herein, shall inure to the State, its successors, assigns, customer agencies, and governmental users of the Deliverables or services.
- e) Except as may be specifically provided in the Statement of Work or elsewhere in this Contract, for any breach of the warranties provided in this Section, the State's exclusive remedy and the Contractor's sole obligation will be limited to:
 - (i) re-performance, repair, or replacement of the nonconforming Deliverable (including without limitation an infringing Deliverable) or service; or
 - (ii) should the State in its sole discretion consent, refund of all amounts paid by the State for the nonconforming Deliverable or service and payment to the State of any additional amounts necessary to equal the State's Cost to Cover. "Cost to Cover" means the cost, properly mitigated, of procuring Deliverables or services of equivalent capability, function, and performance. The payment obligation in subsection (e)(ii) above will not exceed the limits on the Contractor's liability set forth in the Section entitled "Limitation of Liability."
- f) EXCEPT FOR THE EXPRESS WARRANTIES SPECIFIED IN THIS SECTION, THE CONTRACTOR MAKES NO WARRANTIES EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

- 19. SAFETY AND ACCIDENT PREVENTION:** In performing work under this Contract on State premises, the Contractor shall conform to any specific safety requirements contained in the Contract or as required by law or regulation. The Contractor shall take any additional precautions as the State may reasonably require for safety and accident prevention purposes. Any violation of such rules and requirements, unless promptly corrected, shall be grounds for termination of this Contract in accordance with the default provisions hereof.

- 20. INSURANCE:** The Contractor shall maintain all commercial general liability insurance, workers' compensation insurance and any other insurance required under the Contract. The Contractor shall furnish insurance certificate(s) evidencing required insurance coverage acceptable to the State, including endorsements showing the State as an "additional insured" if required under the Contract. Any required endorsements requested by the State must be separately provided; merely referring to such coverage on the certificate(s) is insufficient for this purpose. When performing work on state owned or controlled property, Contractor shall provide a waiver of subrogation in favor of the State for its workers' compensation policy.

21. TERMINATION FOR NON-APPROPRIATION OF FUNDS:

- a) If the term of this Contract extends into fiscal years subsequent to that in which it is approved, such continuation of the Contract is contingent on the appropriation of funds for such purpose by the Legislature. If funds to effect such continued payment are not appropriated, the Contractor agrees to take back any affected Deliverables furnished under this Contract, terminate any services supplied to the State under this Contract, and relieve the State of any further obligation therefor.
- b) The State agrees that if it appears likely that subsection a) above will be invoked, the State and Contractor shall agree to take all reasonable steps to prioritize work and Deliverables and minimize the incurrence of costs prior to the expiration of funding for this Contract.
- c) THE STATE AGREES THAT IF PARAGRAPH a) ABOVE IS INVOKED, COMMERCIAL HARDWARE AND SOFTWARE THAT HAS NOT BEEN PAID FOR SHALL BE RETURNED TO THE CONTRACTOR IN SUBSTANTIALLY THE SAME CONDITION IN WHICH DELIVERED TO THE STATE, SUBJECT TO NORMAL WEAR AND TEAR. THE STATE FURTHER AGREES TO PAY FOR PACKING, CRATING, TRANSPORTATION TO THE CONTRACTOR'S NEAREST FACILITY AND FOR REIMBURSEMENT TO THE CONTRACTOR FOR EXPENSES INCURRED FOR THEIR ASSISTANCE IN SUCH PACKING AND CRATING.
- 22. TERMINATION FOR THE CONVENIENCE OF THE STATE:**
- a) The State may terminate performance of work under this Contract for its convenience in whole or, from time to time, in part, if the Department of General Services, Deputy Director Procurement Division, or designee, determines that a termination is in the State's interest. The Department of General Services, Deputy Director, Procurement Division, or designee, shall terminate by delivering to the Contractor a Notice of Termination specifying the extent of termination and the effective date thereof.
- b) After receipt of a Notice of Termination, and except as directed by the State, the Contractor shall immediately proceed with the following obligations, as applicable, regardless of any delay in determining or adjusting any amounts due under this clause. The Contractor shall:
- (i) Stop work as specified in the Notice of Termination.
 - (ii) Place no further subcontracts for materials, services, or facilities, except as necessary to complete the continuing portion of the Contract.
 - (iii) Terminate all subcontracts to the extent they relate to the work terminated.
 - (iv) Settle all outstanding liabilities and termination settlement proposals arising from the termination of subcontracts;
- c) After termination, the Contractor shall submit a final termination settlement proposal to the State in the form and with the information prescribed by the State. The Contractor shall submit the proposal promptly, but no later than 90 days after the effective date of termination, unless a different time is provided in the Statement of Work or in the Notice of Termination.
- d) The Contractor and the State may agree upon the whole or any part of the amount to be paid as requested under subsection (c) above.
- e) Unless otherwise set forth in the Statement of Work, if the Contractor and the State fail to agree on the amount to be paid because of the termination for convenience, the State will pay the Contractor the following amounts; provided that in no event will total payments exceed the amount payable to the Contractor if the Contract had been fully performed:
- (i) The Contract price for Deliverables or services accepted or retained by the State and not previously paid for, adjusted for any savings on freight and other charges; and
 - (ii) The total of:
 - A) The reasonable costs incurred in the performance of the work terminated, including initial costs and preparatory expenses allocable thereto,
 - but excluding any cost attributable to Deliverables or services paid or to be paid;
- B) The reasonable cost of settling and paying termination settlement proposals under terminated subcontracts that are properly chargeable to the terminated portion of the Contract; and
- C) Reasonable storage, transportation, demobilization, unamortized overhead and capital costs, and other costs reasonably incurred by the Contractor in winding down and terminating its work.
- f) The Contractor will use generally accepted accounting principles, or accounting principles otherwise agreed to in writing by the parties, and sound business practices in determining all costs claimed, agreed to, or determined under this clause.
- 23. TERMINATION FOR DEFAULT:**
- a) The State may, subject to the clause titled "Force Majeure" and to sub-section d) below, by written notice of default to the Contractor, terminate this Contract in whole or in part if the Contractor fails to:
- i) Deliver the Deliverables or perform the services within the time specified in the Contract or any amendment thereto;
 - ii) Make progress, so that the lack of progress endangers performance of this Contract; or
 - iii) Perform any of the other provisions of this Contract.
- b) The State's right to terminate this Contract under sub-section a) above, may be exercised only if the failure constitutes a material breach of this Contract and if the Contractor does not cure such failure within the time frame stated in the State's cure notice, which in no event will be less than fifteen (15) days, unless the Statement of Work calls for a different period.
- c) If the State terminates this Contract in whole or in part pursuant to this Section, it may acquire, under terms and in the manner the Buyer considers appropriate, Deliverables or services similar to those terminated, and the Contractor will be liable to the State for any excess costs for those Deliverables and services, including without limitation costs third party vendors charge for Manufacturing Materials (but subject to the clause entitled "Limitation of Liability"). However, the Contractor shall continue the work not terminated.
- d) If the Contract is terminated for default, the State may require the Contractor to transfer title, or in the case of licensed Software, license, and deliver to the State, as directed by the Buyer, any:
- (i) completed Deliverables,
 - (ii) partially completed Deliverables, and,
 - (iii) subject to provisions of sub-section e) below, Manufacturing Materials related to the terminated portion of this Contract. Nothing in this sub-section d) will be construed to grant the State rights to Deliverables that it would not have received had this Contract been fully performed. Upon direction of the Buyer, the Contractor shall also protect and preserve property in its possession in which the State has an interest.
- e) The State shall pay Contract price for completed Deliverables delivered and accepted and items the State requires the Contractor to transfer under section (d) above. Unless the Statement of Work calls for different procedures or requires no-charge delivery of materials, the Contractor and Buyer shall attempt to agree on the amount of payment for Manufacturing Materials and other materials delivered and accepted by the State for the protection and preservation of the property; provided that where the Contractor has billed the State for any such materials, no additional charge will apply. Failure to agree will constitute a dispute under the Disputes clause. The State may withhold from these amounts any sum it determines to be necessary to protect the State against loss because of outstanding liens or claims of former lien holders.

- the Contractor was not in default, the rights and obligations of the parties shall be the same as if the termination had been issued for the convenience of the State.
- g) Both parties, State and Contractor, upon any termination for default, have a duty to mitigate the damages suffered by it.
- h) The rights and remedies of the State in this clause are in addition to any other rights and remedies provided by law or under this Contract, and are subject to the clause titled "Limitation of Liability."
- 24. FORCE MAJEURE:** Except for defaults of subcontractors at any tier, the Contractor shall not be liable for any excess costs if the failure to perform the Contract arises from causes beyond the control and without the fault or negligence of the Contractor. Examples of such causes include, but are not limited to:
- a) Acts of God or of the public enemy, and
- b) Acts of the federal or State government in either its sovereign or contractual capacity.
- If the failure to perform is caused by the default of a subcontractor at any tier, and if the cause of the default is beyond the control of both the Contractor and subcontractor, and without the fault or negligence of either, the Contractor shall not be liable for any excess costs for failure to perform.
- 25. RIGHTS AND REMEDIES OF STATE FOR DEFAULT:**
- a) In the event any Deliverables furnished or services provided by the Contractor in the performance of the Contract should fail to conform to the requirements herein, or to the sample submitted by the Contractor, the State may reject the same, and it shall become the duty of the Contractor to reclaim and remove the item promptly or to correct the performance of services, without expense to the State, and immediately replace all such rejected items with others conforming to the Contract.
- b) In addition to any other rights and remedies the State may have, the State may require the Contractor, at Contractor's expense, to ship Deliverables via air freight or expedited routing to avoid or minimize actual or potential delay if the delay is the fault of the Contractor.
- c) In the event of the termination of the Contract, either in whole or in part, by reason of default or breach by the Contractor, any loss or damage sustained by the State in procuring any items which the Contractor agreed to supply shall be borne and paid for by the Contractor (but subject to the clause entitled "Limitation of Liability").
- d) The State reserves the right to offset the reasonable cost of all damages caused to the State against any outstanding invoices or amounts owed to the Contractor or to make a claim against the Contractor therefore.
- 26. LIMITATION OF LIABILITY:**
- a) Except as may be otherwise approved by the Department of General Services Deputy Director, Procurement Division or their designee, Contractor's liability for damages to the State for any cause whatsoever, and regardless of the form of action, whether in Contract or in tort, shall be limited to the Purchase Price. For purposes of this sub-section a), "Purchase Price" will mean the aggregate Contract price; except that, with respect to a Contract under which multiple purchase orders will be issued (e.g., a Master Agreement or Multiple Award Schedule contract), "Purchase Price" will mean the total price of the purchase order for the Deliverable(s) or service(s) that gave rise to the loss, such that the Contractor will have a separate limitation of liability for each purchase order.
- b) The foregoing limitation of liability shall not apply (i) to any liability under the General Provisions entitled "Compliance with Statutes and Regulations" (ii) to liability under the General Provisions, entitled "Patent, Copyright, and Trade Secret Indemnity" or to any other liability (including without limitation indemnification obligations) for infringement of third party intellectual property rights; (iii) to claims arising under provisions herein calling for indemnification for third party claims against the State for death, bodily injury to persons or damage to real or tangible personal property caused by the
- or attorney's fees that the State becomes entitled to recover as a prevailing party in any action.
- c) The State's liability for damages for any cause whatsoever, and regardless of the form of action, whether in Contract or in tort, shall be limited to the Purchase Price, as that term is defined in subsection a) above. Nothing herein shall be construed to waive or limit the State's sovereign immunity or any other immunity from suit provided by law.
- d) In no event will either the Contractor or the State be liable for consequential, incidental, indirect, special, or punitive damages, even if notification has been given as to the possibility of such damages, except (i) to the extent that the Contractor's liability for such damages is specifically set forth in the Statement of Work or (ii) to the extent that the Contractor's liability for such damages arises out of subsection b)(i), b)(ii), or b)(iv) above.
- 27. CONTRACTOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY:**
- a) The Contractor shall be liable for damages arising out of injury to the person and/or damage to the property of the State, employees of the State, persons designated by the State for training, or any other person(s) other than agents or employees of the Contractor, designated by the State for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Deliverables either at the Contractor's site or at the State's place of business, provided that the injury or damage was caused by the fault or negligence of the Contractor.
- b) The Contractor shall not be liable for damages arising out of or caused by an alteration or an Attachment not made or installed by the Contractor, or for damage to alterations or Attachments that may result from the normal operation and maintenance of the Deliverables provided by the Contractor during the Contract.
- 28. INDEMNIFICATION:** The Contractor agrees to indemnify, defend and save harmless the State, its officers, agents and employees from any and all third party claims, costs (including without limitation reasonable attorneys' fees), and losses due to the injury or death of any individual, or the loss or damage to any real or tangible personal property, resulting from the willful misconduct or negligent acts or omissions of the Contractor or any of its affiliates, agents, subcontractors, employees, suppliers, or laborers furnishing or supplying work, services, materials, or supplies in connection with the performance of this Contract. Such defense and payment will be conditional upon the following:
- a) The State will notify the Contractor of any such claim in writing and tender the defense thereof within a reasonable time; and
- b) The Contractor will have sole control of the defense of any action on such claim and all negotiations for its settlement or compromise; provided that (i) when substantial principles of government or public law are involved, when litigation might create precedent affecting future State operations or liability, or when involvement of the State is otherwise mandated by law, the State may participate in such action at its own expense with respect to attorneys' fees and costs (but not liability); (ii) where a settlement would impose liability on the State, affect principles of California government or public law, or impact the authority of the State, the Department of General Services will have the right to approve or disapprove any settlement or compromise, which approval will not unreasonably be withheld or delayed; and (iii) the State will reasonably cooperate in the defense and in any related settlement negotiations.
- 29. INVOICES:** Unless otherwise specified, invoices shall be sent to the address set forth herein. Invoices shall be submitted in triplicate and shall include the Contract number; release order number (if applicable); item number; unit price, extended item price and invoice total amount. State sales tax and/or use tax shall be itemized separately and added to each invoice as applicable.

accordance with the provisions of the California Prompt Payment Act, Government Code Section 927 et. seq. Unless expressly exempted by statute, the Act requires State agencies to pay properly submitted, undisputed invoices not more than 45 days after (i) the date of acceptance of Deliverables or performance of services; or (ii) receipt of an undisputed invoice, whichever is later.

31. TAXES: Unless otherwise required by law, the State of California is exempt from Federal excise taxes. The State will only pay for any State or local sales or use taxes on the services rendered or Goods supplied to the State pursuant to this Contract.

32. NEWLY MANUFACTURED GOODS: All Goods furnished under this Contract shall be newly manufactured Goods or certified as new and warranted as new by the manufacturer; used or reconditioned Goods are prohibited, unless otherwise specified.

33. CONTRACT MODIFICATION: No amendment or variation of the terms of this Contract shall be valid unless made in writing, signed by the parties and approved as required. No oral understanding or agreement not incorporated in the Contract is binding on any of the parties.

34. CONFIDENTIALITY OF DATA: All financial, statistical, personal, technical and other data and information relating to the State's operation which are designated confidential by the State and made available to the Contractor in order to carry out this Contract, or which become available to the Contractor in carrying out this Contract, shall be protected by the Contractor from unauthorized use and disclosure through the observance of the same or more effective procedural requirements as are applicable to the State. The identification of all such confidential data and information as well as the State's procedural requirements for protection of such data and information from unauthorized use and disclosure shall be provided by the State in writing to the Contractor. If the methods and procedures employed by the Contractor for the protection of the Contractor's data and information are deemed by the State to be adequate for the protection of the State's confidential information, such methods and procedures may be used, with the written consent of the State, to carry out the intent of this paragraph. The Contractor shall not be required under the provisions of this paragraph to keep confidential any data or information which is or becomes publicly available, is already rightfully in the Contractor's possession without obligation of confidentiality, is independently developed by the Contractor outside the scope of this Contract, or is rightfully obtained from third parties.

35. NEWS RELEASES: Unless otherwise exempted, news releases, endorsements, advertising, and social media content pertaining to this Contract shall not be made without prior written approval of the Department of General Services.

36. DOCUMENTATION:

a) The Contractor agrees to provide to the State, at no charge, all Documentation as described within the Statement of Work, and updated versions thereof, which are necessary or useful to the State in its use of the Equipment or Software provided hereunder. The Contractor agrees to provide additional Documentation at prices not in excess of charges made by the Contractor to its other customers for similar Documentation.

b) If the Contractor is unable to perform maintenance or the State desires to perform its own maintenance on Equipment purchased under this Contract then upon written notice by the State the Contractor will provide at Contractor's then current rates and fees adequate and reasonable assistance including relevant Documentation to allow the State to maintain the Equipment based on the Contractor's methodology. The Contractor agrees that the State may reproduce such Documentation for its own use in maintaining the Equipment. If the Contractor is unable to perform maintenance, the Contractor agrees to license any other Contractor that the State may have hired to maintain the Equipment to use the above noted Documentation. The State agrees to include the Contractor's copyright notice on

copyright instructions to be provided by the Contractor.

37. RIGHTS IN WORK PRODUCT:

- a) All inventions, discoveries, intellectual property, technical communications and records originated or prepared by the Contractor pursuant to this Contract including papers, reports, charts, computer programs, and other Documentation or improvements thereto, and including the Contractor's administrative communications and records relating to this Contract (collectively, the "Work Product"), shall be the Contractor's exclusive property. The provisions of this sub-section a) may be revised in a Statement of Work.
- b) Software and other materials developed or otherwise obtained by or for the Contractor or its affiliates independently of this Contract or applicable purchase order ("Pre-Existing Materials") do not constitute Work Product. If the Contractor creates derivative works of Pre-Existing Materials, the elements of such derivative works created pursuant to this Contract constitute Work Product, but other elements do not. Nothing in this Section 37 will be construed to interfere with the Contractor's or its affiliates' ownership of Pre-Existing Materials.
- c) The State will have Government Purpose Rights to the Work Product as Deliverable or delivered to the State hereunder. "Government Purpose Rights" are the unlimited, irrevocable, worldwide, perpetual, royalty-free, non-exclusive rights and licenses to use, modify, reproduce, perform, release, display, create derivative works from, and disclose the Work Product. "Government Purpose Rights" also include the right to release or disclose the Work Product outside the State for any State government purpose and to authorize recipients to use, modify, reproduce, perform, release, display, create derivative works from, and disclose the Work Product for any State government purpose. Such recipients of the Work Product may include, without limitation, State Contractors, California local governments, the U.S. federal government, and the State and local governments of other states. "Government Purpose Rights" do not include any rights to use, modify, reproduce, perform, release, display, create derivative works from, or disclose the Work Product for any commercial purpose.
- d) The ideas, concepts, know-how, or techniques relating to data processing, developed during the course of this Contract by the Contractor or jointly by the Contractor and the State may be used by either party without obligation of notice or accounting.
- e) This Contract shall not preclude the Contractor from developing materials outside this Contract that are competitive, irrespective of their similarity to materials which might be delivered to the State pursuant to this Contract.

38. SOFTWARE LICENSE: Unless otherwise specified in the Statement of Work, the Contractor hereby grants to the State and the State accepts from the Contractor, subject to the terms and conditions of this Contract, a perpetual, irrevocable, royalty-free, non-exclusive, license to use the Software Products in this Contract (hereinafter referred to as "Software Products").

- a) The State may use the Software Products in the conduct of its own business, and any division thereof
- b) The license granted above authorizes the State to use the Software Products in machine-readable form on the Computer System located at the site(s) specified in the Statement of Work. Said Computer System and its associated units (collectively referred to as CPU) are as designated in the Statement of Work. If the designated CPU is inoperative due to malfunction, the license herein granted shall be temporarily extended to authorize the State to use the Software Products, in machine-readable form, on any other State CPU until the designated CPU is returned to operation.

which the Software Products are to be used provided that the redesignated CPU is substantially similar in size and scale at no additional cost. The redesignation shall not be limited to the original site and will be effective upon the date specified in the notice of redesignation.

- d) Acceptance of Commercial Software (including third party Software) and Custom Software will be governed by the terms and conditions of this Contract.

39. PROTECTION OF PROPRIETARY SOFTWARE AND OTHER PROPRIETARY DATA:

- a) The State agrees that all material appropriately marked or identified in writing as proprietary, and furnished hereunder are provided for the State's exclusive use for the purposes of this Contract only. All such proprietary data shall remain the property of the Contractor. The State agrees to take all reasonable steps to insure that such proprietary data are not disclosed to others, without prior written consent of the Contractor, subject to the California Public Records Act.
- b) The State will insure, prior to disposing of any media, that any licensed materials contained thereon have been erased or otherwise destroyed.
- c) The State agrees that it will take appropriate action by instruction, agreement or otherwise with its employees or other persons permitted access to licensed software and other proprietary data to satisfy its obligations in this Contract with respect to use, copying, modification, protection and security of proprietary software and other proprietary data.

40. RIGHT TO COPY OR MODIFY:

- a) Any Software Product provided by the Contractor in machine-readable form may be copied, in whole or in part, in printed or machine-readable form for use by the State with the designated CPU, to perform one-time benchmark tests, for archival or emergency restart purposes, to replace a worn copy, to understand the contents of such machine-readable material, or to modify the Software Product as provided below; provided, however, that no more than the number of printed copies and machine-readable copies as specified in the Statement of Work will be in existence under this Contract at any time without prior written consent of the Contractor. Such consent shall not be unreasonably withheld by the Contractor. The original, and any copies of the Software Product, in whole or in part, which are made hereunder shall be the property of the Contractor.
- b) The State may modify any non-personal computer Software Product, in machine-readable form, for its own use and merge it into other program material. Any portion of the Software Product included in any merged program material shall be used only on the designated CPUs and shall be subject to the terms and conditions of the Contract.

41. FUTURE RELEASES: Unless otherwise specifically provided in this Contract, or the Statement of Work, if improved versions, e.g., patches, bug fixes, updates or releases, of any Software Product are developed by the contractor, and are made available to other licensees, they will be made available to the State at no additional cost only if such are made available to other licensees at no additional cost. If the Contractor offers new versions or upgrades to the Software Product, they shall be made available to the State at the State's option at a price no greater than the Contract price plus a price increase proportionate to the increase from the list price of the original version to that of the new version, if any. If the Software Product has no list price, such price increase will be proportionate to the increase in average price from the original to the new version, if any, as estimated by the Contractor in good faith.

42. ENCRYPTION/CPU ID AUTHORIZATION CODES:

- a) When Encryption/CPU Identification (ID) authorization codes are required to operate the Software Products, the

the Software.

- b) In case of an inoperative CPU, the Contractor will provide a temporary encryption/CPU ID authorization code to the State for use on a temporarily authorized CPU until the designated CPU is returned to operation.
- c) When changes in designated CPUs occur, the State will notify the Contractor via telephone and/or facsimile/e-mail of such change. Upon receipt of such notice, the Contractor will issue via telephone and/or facsimile/e-mail to the State within 24 hours, a temporary encryption ID authorization code for use on the newly designated CPU until such time as permanent code is assigned.

43. PATENT, COPYRIGHT AND TRADE SECRET INDEMNITY:

- a) Contractor will indemnify, defend, and save harmless the State, its officers, agents, and employees, from any and all third party claims, costs (including without limitation reasonable attorneys' fees), and losses for infringement or violation of any U.S. Intellectual Property Right by any product or service provided hereunder. With respect to claims arising from computer Hardware or Software manufactured by a third party and sold by Contractor as a reseller, Contractor will pass through to the State such indemnity rights as it receives from such third party ("Third Party Obligation") and will cooperate in enforcing them; provided that if the third party manufacturer fails to honor the Third Party Obligation, Contractor will provide the State with indemnity protection equal to that called for by the Third Party Obligation, but in no event greater than that called for in the first sentence of this Section . The provisions of the preceding sentence apply only to third party computer Hardware or Software sold as a distinct unit and accepted by the State.

Unless a Third Party Obligation provides otherwise, the defense and payment obligations set forth in this Section will be conditional upon the following:

- (i) The State will notify the Contractor of any such claim in writing and tender the defense thereof within a reasonable time; and
- (ii) The Contractor will have sole control of the defense of any action on such claim and all negotiations for its settlement or compromise; provided that (a) when substantial principles of government or public law are involved, when litigation might create precedent affecting future State operations or liability, or when involvement of the State is otherwise mandated by law, the State may participate in such action at its own expense with respect to attorneys' fees and costs (but not liability); (b) where a settlement would impose liability on the State, affect principles of California government or public law, or impact the authority of the State, the Department of General Services will have the right to approve or disapprove any settlement or compromise, which approval will not unreasonably be withheld or delayed; and (c) the State will reasonably cooperate in the defense and in any related settlement negotiations.
- b) Should the Deliverables, or the operation thereof, become, or in the Contractor's opinion are likely to become, the subject of a claim of infringement or violation of a U.S. Intellectual Property Right, the State shall permit the Contractor, at its option and expense, either to procure for the State the right to continue using the Deliverables, or to replace or modify the same so that they become non-infringing. If none of these options can reasonably be taken, or if the use of such Deliverables by the State shall be prevented by injunction, the Contractor agrees to take back such Deliverables and make every reasonable effort to assist the State in procuring substitute Deliverables. If, in the sole opinion of the State, the return of such

infringing Deliverables makes the retention of other Deliverables acquired from the Contractor under this Contract impractical, the State shall then have the option of terminating such Contracts, or applicable portions thereof, without penalty or termination charge. The Contractor agrees to take back such Deliverables and refund any sums the State has paid the Contractor less any reasonable amount for use or damage.

- c) The Contractor shall have no liability to the State under any provision of this clause with respect to any claim of patent, copyright or trade secret infringement which is based upon:
 - (i) The combination or utilization of Deliverables furnished hereunder with Equipment, Software or devices not made or furnished by the Contractor; or,
 - (ii) The operation of Equipment furnished by the Contractor under the control of any Operating Software other than, or in addition to, the current version of Contractor-supplied Operating Software; or
 - (iii) The modification initiated by the State, or a third party at the State's direction, of any Deliverable furnished hereunder; or
 - (iv) The combination or utilization of Software furnished hereunder with non-contractor supplied Software.
- d) The Contractor certifies that it has appropriate systems and controls in place to ensure that State funds will not be used in the performance of this Contract for the acquisition, operation or maintenance of computer Software in violation of copyright laws.

44. DISPUTES:

- a) The parties shall deal in good faith and attempt to resolve potential disputes informally. If the dispute persists, the Contractor shall submit to the contracting Department Director or designee a written demand for a final decision regarding the disposition of any dispute between the parties arising under, related to or involving this Contract. Contractor's written demand shall be fully supported by factual information, and if such demand involves a cost adjustment to the Contract, the Contractor shall include with the demand a written statement signed by an authorized person indicating that the demand is made in good faith, that the supporting data are accurate and complete and that the amount requested accurately reflects the Contract adjustment for which Contractor believes the State is liable. The contracting Department Director or designee shall have 30 days after receipt of Contractor's written demand invoking this Section "Disputes" to render a written decision. If a written decision is not rendered within 30 days after receipt of the Contractor's demand, it shall be deemed a decision adverse to the Contractor's contention. If the Contractor is not satisfied with the decision of the contracting Department Director or designee, the Contractor may appeal the decision, in writing, within 15 days of its issuance (or the expiration of the 30 day period in the event no decision is rendered by the contracting department), to the Department of General Services, Deputy Director, Procurement Division, who shall have 45 days to render a final decision. If the Contractor does not appeal the decision of the contracting Department Director or designee, the decision shall be conclusive and binding regarding the dispute and the Contractor shall be barred from commencing an action in court, or with the Victims Compensation Government Claims Board, for failure to exhaust Contractor's administrative remedies.
- b) Pending the final resolution of any dispute arising under, related to or involving this Contract, Contractor agrees to diligently proceed with the performance of this Contract, including the delivery of Goods or providing of services in accordance with the State's instructions regarding this Contract. Contractor's failure to diligently proceed in accordance with the State's instructions regarding this Contract shall be considered a material breach of this Contract.

- c) Any final decision of the State shall be expressly identified as such, shall be in writing, and shall be signed by the Deputy Director, Procurement Division if an appeal was made. If the Deputy Director, Procurement Division fails to render a final decision within 45 days after receipt of the Contractor's appeal for a final decision, it shall be deemed a final decision adverse to the Contractor's contentions. The State's final decision shall be conclusive and binding regarding the dispute unless the Contractor commences an action in a court of competent jurisdiction to contest such decision within 90 days following the date of the final decision or one (1) year following the accrual of the cause of action, whichever is later.
- d) For disputes involving purchases made by the Department of General Services, Procurement Division, the Contractor shall submit to the Department Director or designee a written demand for a final decision, which shall be fully supported in the manner described in subsection a above. The Department Director or designee shall have 30 days to render a final decision. If a final decision is not rendered within 30 days after receipt of the Contractor's demand, it shall be deemed a final decision adverse to the Contractor's contention. The final decision shall be conclusive and binding regarding the dispute unless the Contractor commences an action in a court of competent jurisdiction to contest such decision within 90 days following the date of the final decision or one (1) year following the accrual of the cause of action, whichever is later.
- e) The dates of decision and appeal in this section may be modified by mutual consent, as applicable, excepting the time to commence an action in a court of competent jurisdiction.

45. STOP WORK:

- a) The State may, at any time, by written Stop Work Order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this Contract for a period up to 45 days after the Stop Work Order is delivered to the Contractor, and for any further period to which the parties may agree. The Stop Work Order shall be specifically identified as such and shall indicate it is issued under this clause. Upon receipt of the Stop Work Order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the Stop Work Order during the period of work stoppage. Within a period of 45 days after a Stop Work Order is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the State shall either:
 - (i) Cancel the Stop Work Order; or
 - (ii) Terminate the work covered by the Stop Work Order as provided for in the termination for default or the termination for convenience clause of this Contract.
- b) If a Stop Work Order issued under this clause is canceled or the period of the Stop Work Order or any extension thereof expires, the Contractor shall resume work. The State shall make an equitable adjustment in the delivery schedule, the Contract price, or both, and the Contract shall be modified, in writing, accordingly, if:
 - (i) The Stop Work Order results in an increase in the time required for, or in the Contractor's cost properly allocable to the performance of any part of this Contract; and
 - (ii) The Contractor asserts its right to an equitable adjustment within 60 days after the end of the period of work stoppage; provided, that if the State decides the facts justify the action, the State may receive and act upon a proposal submitted at any time before final payment under this Contract.
- c) If a Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated in accordance with the provision entitled Termination for the Convenience of the State, the State shall allow reasonable costs resulting from the Stop Work Order in arriving at the termination settlement.

- d) The State shall not be liable to the Contractor for loss of profits because of a Stop Work Order issued under this clause.
- 46. EXAMINATION AND AUDIT:** The Contractor agrees that the State or its designated representative shall have the right to review and copy any records and supporting documentation directly pertaining to performance of this Contract. The Contractor agrees to maintain such records for possible audit for a minimum of three (3) years after final payment, unless a longer period of records retention is stipulated. The Contractor agrees to allow the auditor(s) access to such records during normal business hours and in such a manner so as to not interfere unreasonably with normal business activities and to allow interviews of any employees or others who might reasonably have information related to such records. Further, the Contractor agrees to include a similar right of the State to audit records and interview staff in any subcontract related to performance of this Contract. The State shall provide reasonable advance written notice of such audit(s) to the Contractor.
- 47. FOLLOW-ON CONTRACTS:**
- a) If the Contractor or its affiliates provides Technical Consulting and Direction (as defined below), the Contractor and its affiliates:
 - (i) will not be awarded a subsequent Contract to supply the service or system, or any significant component thereof, that is used for or in connection with any subject of such Technical Consulting and Direction; and
 - (ii) will not act as consultant to any person or entity that does receive a Contract described in sub-section (i). This prohibition will continue for one (1) year after termination of this Contract or completion of the Technical Consulting and Direction, whichever comes later.
 - b) "Technical Consulting and Direction" means services for which the Contractor received compensation from the State and includes:
 - (i) development of or assistance in the development of work statements, specifications, solicitations, or feasibility studies;
 - (ii) development or design of test requirements;
 - (iii) evaluation of test data;
 - (iv) direction of or evaluation of another Contractor;
 - (v) provision of formal recommendations regarding the acquisition of Information Technology products or services; or
 - (vi) provisions of formal recommendations regarding any of the above. For purposes of this Section, "affiliates" are employees, directors, partners, joint venture participants, parent corporations, subsidiaries, or any other entity controlled by, controlling, or under common control with the Contractor. Control exists when an entity owns or directs more than fifty percent (50%) of the outstanding shares or securities representing the right to vote for the election of directors or other managing authority.
 - c) To the extent permissible by law, the Director of the Department of General Services, or designee, may waive the restrictions set forth in this Section by written notice to the Contractor if the Director determines their application would not be in the State's best interest. Except as prohibited by law, the restrictions of this Section will not apply:
 - (i) to follow-on advice given by vendors of commercial off-the-shelf products, including Software and Hardware, on the operation, integration, repair, or maintenance of such products after sale; or
 - (ii) where the State has entered into a master agreement for Software or services and the scope of work at the time of Contract execution expressly calls for future recommendations among the Contractor's own products.
 - d) The restrictions set forth in this Section are in addition to conflict of interest restrictions imposed on public Contractors
- by California law ("Conflict Laws"). In the event of any inconsistency, such Conflict Laws override the provisions of this Section, even if enacted after execution of this Contract.
- 48. PRIORITY HIRING CONSIDERATIONS:** If this Contract includes services in excess of \$200,000, the Contractor shall give priority consideration in filling vacancies in positions funded by the Contract to qualified recipients of aid under Welfare and Institutions Code Section 11200 in accordance with PCC Section 10353.
- 49. COVENANT AGAINST GRATUITIES:** The Contractor warrants that no gratuities (in the form of entertainment, gifts, or otherwise) were offered or given by the Contractor, or any agent or representative of the Contractor, to any officer or employee of the State with a view toward securing the Contract or securing favorable treatment with respect to any determinations concerning the performance of the Contract. For breach or violation of this warranty, the State shall have the right to terminate the Contract, either in whole or in part, and any loss or damage sustained by the State in procuring on the open market any items which the Contractor agreed to supply shall be borne and paid for by the Contractor. The rights and remedies of the State provided in this clause shall not be exclusive and are in addition to any other rights and remedies provided by law or in equity.
- 50. NONDISCRIMINATION CLAUSE:**
- a) During the performance of this Contract, the Contractor and its subcontractors shall not unlawfully discriminate, harass or allow harassment, against any employee or applicant for employment because of sex, sexual orientation, race, color, ancestry, religious creed, national origin, disability (including HIV and AIDS), medical condition (cancer), age, marital status, and denial of family care leave. The Contractor and subcontractors shall insure that the evaluation and treatment of their employees and applicants for employment are free from such discrimination and harassment. The Contractor and subcontractors shall comply with the provisions of the Fair Employment and Housing Act (Government Code, Section 12990 et seq.) and the applicable regulations promulgated thereunder (California Code of Regulations, Title 2, Section 7285.0 et seq.). The applicable regulations of the Fair Employment and Housing Commission implementing Government Code Section 12990 (a-f), set forth in Chapter 5 of Division 4 of Title 2 of the California Code of Regulations are incorporated into this Contract by reference and made a part hereof as if set forth in full. The Contractor and its subcontractors shall give written notice of their obligations under this clause to labor organizations with which they have a collective bargaining or other agreement.
 - b) The Contractor shall include the nondiscrimination and compliance provisions of this clause in all subcontracts to perform work under the Contract.
- 51. NATIONAL LABOR RELATIONS BOARD CERTIFICATION:** The Contractor swears under penalty of perjury that no more than one final, unappealable finding of contempt of court by a federal court has been issued against the Contractor within the immediately preceding two-year period because of the Contractor's failure to comply with an order of the National Labor Relations Board. This provision is required by, and shall be construed in accordance with, PCC Section 10296.
- 52. ASSIGNMENT OF ANTITRUST ACTIONS:** Pursuant to Government Code Sections 4552, 4553, and 4554, the following provisions are incorporated herein:
- a) In submitting a bid to the State, the supplier offers and agrees that if the bid is accepted, it will assign to the State all rights, title, and interest in and to all causes of action it may have under Section 4 of the Clayton Act (15 U.S.C. 15) or under the Cartwright Act (Chapter 2, commencing with Section 16700, of Part 2 of Division 7 of the Business and Professions Code), arising from purchases of Goods, material or other items, or services by the supplier for sale to the State pursuant to the solicitation. Such assignment shall

- be made and become effective at the time the State tenders final payment to the supplier.
- b) If the State receives, either through judgment or settlement, a monetary recovery for a cause of action assigned under this chapter, the assignor shall be entitled to receive reimbursement for actual legal costs incurred and may, upon demand, recover from the State any portion of the recovery, including treble damages, attributable to overcharges that were paid by the assignor but were not paid by the State as part of the bid price, less the expenses incurred in obtaining that portion of the recovery.
- c) Upon demand in writing by the assignor, the assignee shall, within one year from such demand, reassign the cause of action assigned under this part if the assignor has been or may have been injured by the violation of law for which the cause of action arose and
- (i) the assignee has not been injured thereby, or
- (ii) the assignee declines to file a court action for the cause of action.
- 53. DRUG-FREE WORKPLACE CERTIFICATION:** The Contractor certifies under penalty of perjury under the laws of the State of California that the Contractor will comply with the requirements of the Drug-Free Workplace Act of 1990 (Government Code Section 8350 et seq.) and will provide a drug-free workplace by taking the following actions:
- a) Publish a statement notifying employees that unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance is prohibited and specifying actions to be taken against employees for violations, as required by Government Code Section 8355(a).
- b) Establish a Drug-Free Awareness Program as required by Government Code Section 8355(b) to inform employees about all of the following:
- (i) the dangers of drug abuse in the workplace;
- (ii) the person's or organization's policy of maintaining a drug-free workplace;
- (iii) any available counseling, rehabilitation and employee assistance programs; and,
- (iv) penalties that may be imposed upon employees for drug abuse violations.
- c) Provide, as required by Government Code Section 8355(c), that every employee who works on the proposed or resulting Contract:
- (i) will receive a copy of the company's drug-free policy statement; and,
- (ii) will agree to abide by the terms of the company's statement as a condition of employment on the Contract.
- 54. FOUR-DIGIT DATE COMPLIANCE:** Contractor warrants that it will provide only Four-Digit Date Compliant (as defined below) Deliverables and/or services to the State. "Four Digit Date Compliant" Deliverables and services can accurately process, calculate, compare, and sequence date data, including without limitation date data arising out of or relating to leap years and changes in centuries. This warranty and representation is subject to the warranty terms and conditions of this Contract and does not limit the generality of warranty obligations set forth elsewhere herein.
- 55. SWEATFREE CODE OF CONDUCT:**
- a) Contractor declares under penalty of perjury that no equipment, materials, or supplies furnished to the State pursuant to the Contract have been produced in whole or in part by sweatshop labor, forced labor, convict labor, indentured labor under penal sanction, abusive forms of child labor or exploitation of children in sweatshop labor, or with the benefit of sweatshop labor, forced labor, convict labor, indentured labor under penal sanction, abusive forms of child labor or exploitation of children in sweatshop labor. The Contractor further declares under penalty of perjury that they adhere to the Sweatfree Code of Conduct as set forth on the California Department of Industrial Relations website located at www.dir.ca.gov, and Public Contract Code Section 6108.
- b) The Contractor agrees to cooperate fully in providing reasonable access to its records, documents, agents or employees, or premises if reasonably required by authorized officials of the State, the Department of Industrial Relations, or the Department of Justice to determine the Contractor's compliance with the requirements under paragraph (a).
- 56. RECYCLED CONTENT REQUIREMENTS:** The Contractor shall certify in writing under penalty of perjury, the minimum, if not exact, percentage of post-consumer material (as defined in the Public Contract Code (PCC) Section 12200-12209), in products, materials, goods, or supplies offered or sold to the State that fall under any of the statutory categories regardless of whether the product meets the requirements of Section 12209. The certification shall be provided by the contractor, even if the product or good contains no postconsumer recycled material, and even if the postconsumer content is unknown. With respect to printer or duplication cartridges that comply with the requirements of Section 12156(e), the certification required by this subdivision shall specify that the cartridges so comply (PCC 12205 (b)(2)). A state agency contracting officer may waive the certification requirements if the percentage of postconsumer material in the products, materials, goods, or supplies can be verified in a written advertisement, including, but not limited to, a product label, a catalog, or a manufacturer or vendor Internet web site. Contractors are to use, to the maximum extent economically feasible in the performance of the contract work, recycled content products (PCC 12203(d)).
- 57. CHILD SUPPORT COMPLIANCE ACT:** For any Contract in excess of \$100,000, the Contractor acknowledges in accordance with PCC Section 7110, that:
- a) The Contractor recognizes the importance of child and family support obligations and shall fully comply with all applicable State and federal laws relating to child and family support enforcement, including, but not limited to, disclosure of information and compliance with earnings assignment orders, as provided in Chapter 8 (commencing with Section 5200) of Part 5 of Division 9 of the Family Code; and
- b) The Contractor, to the best of its knowledge is fully complying with the earnings assignment orders of all employees and is providing the names of all new employees to the New Hire Registry maintained by the California Employment Development Department.
- 58. AMERICANS WITH DISABILITIES ACT:** The Contractor assures the State that the Contractor complies with the Americans with Disabilities Act of 1990 (42 U.S.C. 12101 et seq.).
- 59. ELECTRONIC WASTE RECYCLING ACT OF 2003:** The Contractor certifies that it complies with the applicable requirements of the Electronic Waste Recycling Act of 2003, Chapter 8.5, Part 3 of Division 30, commencing with Section 42460 of the Public Resources Code. The Contractor shall maintain documentation and provide reasonable access to its records and documents that evidence compliance.
- 60. USE TAX COLLECTION:** In accordance with PCC Section 10295.1, the Contractor certifies that it complies with the requirements of Section 7101 of the Revenue and Taxation Code. Contractor further certifies that it will immediately advise the State of any change in its retailer's seller's permit or certification of registration or applicable affiliate's seller's permit or certificate of registration as described in subdivision (a) of PCC Section 10295.1.
- 61. EXPATRIATE CORPORATIONS:** Contractor hereby declares that it is not an expatriate corporation or subsidiary of an expatriate corporation within the meaning of PCC Sections 10286 and 10286.1, and is eligible to contract with the State.
- 62. DOMESTIC PARTNERS:** For contracts over \$100,000 executed or amended after January 1, 2007, the contractor certifies that the contractor is in compliance with Public Contract Code Section 10295.3.

63. SMALL BUSINESS PARTICIPATION AND DVBE PARTICIPATION REPORTING REQUIREMENTS:

- a) If for this Contract the Contractor made a commitment to achieve small business participation, then the Contractor must within 60 days of receiving final payment under this Contract (or within such other time period as may be specified elsewhere in this Contract) report to the awarding department the actual percentage of small business participation that was achieved. (Govt. Code § 14841.)
 - b) If for this Contract the Contractor made a commitment to achieve disabled veteran business enterprise (DVBE) participation, then Contractor must within 60 days of receiving final payment under this Contract (or within such other time period as may be specified elsewhere in this Contract) certify in a report to the awarding department: (1) the total amount the prime Contractor received under the Contract; (2) the name and address of the DVBE(s) that participated in the performance of the Contract; (3) the amount each DVBE received from the prime Contractor; (4) that all payments under the Contract have been made to the DVBE; and (5) the actual percentage of DVBE participation that was achieved. A person or entity that knowingly provides false information shall be subject to a civil penalty for each violation. (Mil. & Vets. Code § 999.5(d); Govt. Code § 14841.)
- 64. LOSS LEADER:** It is unlawful for any person engaged in business within this state to sell or use any article or product as a "loss leader" as defined in Section 17030 of the Business and Professions Code. (PCC 12104.5(b).).



William Campos

Summary of Experience and Qualifications

William has worked Deloitte's Government Public Services (GSP) practice since 2014 under the Cybersecurity & Strategic Risk practice. William has experience assessing information security programs against industry leading practices such as NIST 800-53 and PCI-DSS, to identify weaknesses and provide recommendations to strengthen their programs. His knowledge with NIST based frameworks has allowed him assist State agencies to assess, document, and mature their Security & Privacy controls to receive compliance accreditation(s) for systems with a total cost of 906 M.

Deloitte Experience

Industry: Government Sector: State, Local, and Higher Ed

Offering Portfolio: Cyber and Strategic Risk Offering: Cyber Strategy

Competency Area: Technology

Enter your Role; 22 months.

State of California Office of Systems Integration (OSI)

The Health Benefit Exchange (HBEX) serves as the healthcare enrollment and eligibility for Citizens of California. This project required in-depth knowledge of security compliance requirements for State exchanges to include Centers for Medicare and Medicaid Services (CMS) and/or Internal Revenue Service (IRS); both based on NIST 800-53. This required documenting the respective remediation plans and remediation efforts to regularly report updates to CMS and IRS.

Assisted with security design requirements to modernize the system from a co-located data center to a cloud hosted environment to align with regulatory compliance requirements and prepare for re-certification. This included identifying requirements to perform automated scans (using Nessus) and harden the information system as per regulatory requirements.

Role: Compliance Lead

Technical Environment:

Hybrid: Co-located on-prem data centers and Amazon Web Services (AWS) cloud environments

Industry: Government Sector: State, Local, and Higher Ed

Offering Portfolio: Cyber and Strategic Risk Offering: Cyber Strategy

Competency Area: Technology

Enter your Role; 10 months.

State of Wyoming - WINGS

Supported a State agency in their Medicaid Management Information System (MMIS) modernization efforts, by assessing their cloud hosted System Integration (SI) and Data Warehouse (DW) modules against CMS standards (NIST based), documenting their System Security Plan (SSP), and developed the POA&M to strategize remediation efforts for security for security control gaps. This also included developing Business Continuity and Disaster Recovery Plans, to ensure that both strategic and technical capabilities are in place to support business operations and assist with system recovery efforts in the event of a disaster.

Role: Compliance Lead

Technical Environment: AWS and Azure cloud environments

Industry: Government **Sector:** State, Local, and Higher Ed

Offering Portfolio: Cyber and Strategic Risk **Offering:** Cyber Strategy

Competency Area: Technology

Enter your Role: 24 months.

State Agency

Integrated Eligibility System

Supported a State agency with completing their System Security Plan (SSP) to achieve Certification and Accreditation from CMS and IRS, by assessing existing security governance practices and controls. Coordinated with the State Agency to plan and execute the CMS and IRS authorization review processes, which included coordinating with Agency officials and independent assessors to walkthrough the system's security posture and validate the effectiveness of security controls.

Role: Compliance Lead

Technical Environment: On-prem co-located data centers

System Experience

Software / Products: Project experience in assessing on-prem and cloud hosted environments.

Education

Enter the Bachelors Degree(s) and major (e.g. Bachelor of Arts, Finance)

Bachelor of Business Administration in Management Information Systems

Professional Affiliations / Certifications

- Certified Information Systems Auditor (CISA) - ISACA

Deloitte.

Lenin Vyas

Summary

Lenin has more than 16 years of experience managing large, complex, digital projects. He applies SDLC processes, Project Management standards, as well as his deep expertise in managing Application Architecture, Analysis, Design, Development and Testing methodologies. He has managed global delivery teams consisting of 150-200 practitioners working on various platforms such as Salesforce, AWS, Azure DevOps, .Net, Java, Python, FileNet, Mobile Apps, Business Intelligence, MS Dynamics CRM, SQL / Oracle / DB2 Servers etc. For the past several years, Lenin has applied his understanding of client's business in the areas of scope management, risk management and issue resolution. He has cross domain knowledge of Commercial as well as Public Sector clients especially in the areas of Health and Human Services, Labor, and Pensions. Some of his marquee clients while working at Deloitte include Google LLC, PA Liquor Control Board, Governments of CA, IL, OH, AZ, AL, WV, MA and Washington DC.

Deloitte Experience

Project: Recruitment Portal, City and County of San Francisco (CCSF)

Role: Technical Project Manager; 1 month.

CCSF contracted Deloitte to design and implement a cloud based portal that integrates with their existing Smart Recruiters system. The new portal is designed to enable city and county recruiters assess various applicants on a variety of metrics. The new portal enables recruiters to understand candidates' qualification in terms of education, past experiences, as well as test scores to help identify top candidates using streamlined statistical methods.

Responsibilities: Lenin worked as Technical Project Manager managing a team of Deloitte professionals to deliver a stable cloud based system.

- Analyze project scope and requirements
- Develop project management plan
- Manage scope, timelines and staffing
- Manage day to day functioning of a team consisting of business analysts, backend / front-end developers, functional testers, performance testers, and cloud DevOps engineers
- Manage various testing phases, resolve technical and service incidents
- Identify risks, propose mitigation plans, present them to various stakeholders
- Track and monitor progress per the plan
- Coordinate security testing efforts
- Mitigate identified security issues
- Manage infrastructure readiness, contingency planning, and go-live checklist
- Conduct performance reviews of various team members

Technical Environment: AWS, Python, JIRA, PostgreSQL.

Project / Client: COVID-19 Initiatives, California Department of Public Health (CDPH)

Role: Technical Advisor; 5.5 months.

CDPH contracted Deloitte to provide Technical Advisory / Project Management services for various key initiatives. These initiatives primarily included working directly with third party vendors, and CDPH technical and business leadership to resolve critical COVID-19 related tasks. For example, Deloitte worked with third party vendor and CDPH team to provide technical advisory services during CalREDIE SQL Server migration project. Deloitte also worked with various teams and county stakeholders to coordinate activities related to providing COVID-19 related data from CalREDIE for faster consumption. Additionally, Deloitte was also contracted to provide Technical Advisory / Project Management services to help resolve critical issues related to CAIR2.

Deloitte

Responsibilities: Lenin worked as Technical Advisor managing coordination between third party vendors, office of CIO, various counties, and CDPH technical and business teams to resolve critical COVID-19 related initiatives.

- Understand and analyze existing system issues
- Work with the existing vendor and CDPH teams to identify various approaches to resolve architectural and business issues
- Coordinate with various stakeholders to derive project management plan, timelines, and resources
- Identify risks, propose mitigation plans, present them to various stakeholders, and arrive at consensus
- Track and monitor progress per the plan
- Oversee execution of the plan
- Manage / Participate in meetings to manage scope, and timelines
- Provide inputs to executives for better decision making
- Manage development of data migration plan, performance testing, batch scheduling, infrastructure readiness, contingency plan, and go-live checklist related activities
- Manage post go-live activities through analysis and resolution of business / technical incidents
- Coordinate with vendor on future technical upgrade roadmap

Technical Environment: SQL Server, Java, Oracle.

Project: State of IL & OH Pandemic Unemployment Assistance

Role: Center Delivery Manager; 4 months.

States of Illinois and Ohio contracted Deloitte to implement a Microsoft .Net and AWS Cloud based system that enables citizens who lost their earnings due to COVID 19 to file for unemployment insurance claims, calculates their eligibility, issues benefit payments and allows staff to track the claim's lifecycle. The new AWS / .Net based system was conceived and deployed to production in a record short cycle lasting only few weeks and is currently under maintenance and operations.

Responsibilities: Lenin worked as Center Delivery Manager managing a team of practitioners consisting of developers, testers, and DevOps practitioners.

- Understand new legislation related to Pandemic Unemployment Assistance
- Work with the existing product team to understand AWS / .Net architecture
- Lead staff augmentation and lay down processes for tracking requirements, design items, work allocation and tracking using Azure DevOps
- Understand business / technical requirements and scope of work to be delivered in a fast paced delivery schedule
- Identify risks, escalate to leadership and create project work plan
- Work with Cloud Managed Service team to setup AWS environments, and DevOps processes
- Manage staff ramp-up / ramp-down schedules
- Manage various service level agreements (SLAs)
- Coordinate security testing efforts and mitigate any issues identified
- Manage infrastructure readiness, contingency planning, and go-live readiness
- Identify risks, issues and provide mitigation plans
- Perform team appraisals and build and develop practitioners
- Provide inputs to executives for better decision making

Deloitte

- Manage post go-live activities including service ticket resolutions and potential technical optimization and upgrades

Technical Environment: AWS, .Net, Oracle, Azure DevOps.

Project: Sales & Marketing Salesforce Modernization, Google LLC

Role: Center Delivery Manager; 9 months.

Google contracted Deloitte to migrate and enhance its classic Salesforce system that it uses to manage Sales and Marketing portfolios to a newly upgraded Salesforce application. The new system enables management of various functionalities such as tracking Sales pipeline, Marketing opportunities, Account Hierarchy at regional and global level. The initial transition from classic to latest Salesforce platform went live in mid-2019 and Deloitte continues to enhance the system to meet Google's evolving Cloud strategy.

Responsibilities: Lenin worked as a Center Delivery Manager (CDM) managing multiple Scrum Teams consisting of Salesforce developers, testers and DevOps practitioners. He managed project delivery thru teams working in Deloitte US Delivery Centers while coordinating with Deloitte as well as Google practitioners working at client location in Sunnyvale, CA.

- Lead staff augmentation and lay down processes for work assignment and tracking
- Understand requirements and agreed upon scope
- Manage delivery per the scope and timelines
- Manage staff ramp-up / ramp-down schedules
- Maintain business relationship with client counterparts from Google including Technical Leads
- Identify risks, issues and provide mitigation plans
- Participate in Agile ceremonies such as stand up meetings, sprint planning, sprint backlog refinement, sprint review meetings etc
- Monitor and report development and quality assurance tasks
- Participate in Deloitte and client meetings to manage scope, budget and timelines
- Manage various testing phases, go-live readiness, and post go-live service level agreements (SLAs) through issue resolution and technical upgrades
- Perform team appraisals and build and develop practitioners

Technical Environment: Salesforce Service Cloud, JIRA, Confluence.

Project: AZ Department of Financial Institutions (DFI) eLicensing

Role: Project Manager; 10 months.

DFI contracted Deloitte to implement a new eLicensing system using Salesforce. The new system enables citizens to apply and / or renew businesses licenses, pay fees, penalties as well as complete relevant business processes. It also consists of a back office portal that enables staff to process license applications, identify / investigate compliants, calculate penalties, issue notices, generate correspondences, accept fees, and manage case lifecycle. Project went live in March 2019 and Deloitte continued to provide hypercare before transitioning the maintenance of the system to State IT department.

Responsibilities: Lenin was a Project Manager working between US Delivery Center and client site in Phoenix, AZ. He managed delivery of Salesforce implementation thru a team based at client site, offsite and offshore.

- Manage Project Work Plan
- Manage Scope and Design sessions

Deloitte

- Participate in Agile ceremonies such as stand up meetings, sprint planning, sprint backlog refinement, sprint review meetings etc
- Monitor and report development and quality assurance tasks
- Identify risks, issues and provide mitigation plans
- Manage various testing phases, data migration, go-live readiness, system cutover, and post go-live incidents through issue resolution and technical upgrades
- Participate in Executive Committee meetings and work with client's executives to manage scope, budget and timelines
- Perform team appraisals and build and develop practitioners
- Manage raising invoices and coordinate with client's executives for payment receivables

Technical Environment: Salesforce Service Cloud, JIRA.

Project: The Retirement Systems of Alabama (RSA) & The West Virginia Consolidated Public Retirement Board (CPRB)

Role: Project Manager & Group Delivery Manager; 43 months.

RSA and CPRB contracted Deloitte to design and implement a new pension administration system for their respective public sector employees such as educational employees, judges, sheffirs etc. Between 2014 through 2019, Deloitte successfully deployed agencywide separate web-based systems for both the states, and is currently maintaining it. This new system replaces specific functionalities of legacy mainframe system, providing more efficiency in citizen Self-Service, Customer Relationship Management (MS Dynamics CRM), Workflow management, Master Data Management and Correspondence generation.

Responsibilities: Lenin worked as a Project Manager at client site in Montgomery, AL from November 2017 thru July 2018. Prior to that, he worked as a Group Delivery Manager from Deloitte's India based delivery centers. He was responsible for managing delivery by a high performing global team consisting of 150+ practitioners working across multiple locations for both AL and WV pension administration systems.

- Plan Project Delivery Schedule across multiple go-live phases for both states
- Staff augmentation, training and development across multiple locations
- Develop processes for assignment, monitoring and reporting of tasks
- Identify risks, issues and provide mitigation plans
- Work with client executive team to manage scope, budget and timelines
- Implement quality control processes and perform audits
- Manage various testing phases, multi-phase go-lives, system maintenance and operations through ticket resolution and technical optimizations
- Disaster recovery planning
- Leverage resources and best practices across multiple projects under same business domain
- Perform team appraisals and build and develop practitioners

Technical Environment: .Net, SQL Server, IBM FileNet, Team Foundation Server, MS Dynamics.

Project: Massachusetts Unemployment Insurance System (UI Online)

Role: Project Manager; 34 months.

Department of Unemployment Assistance (DUA) of MA administers the Unemployment Insurance (UI) program. DUA contracted Deloitte to design, develop and implement a web-based Unemployment

Deloitte

Insurance system, called UI Online, to better serve customers. UI Online expedites UI payments to unemployed workers and provide all users with many convenient, online services.

Responsibilities: Lenin worked in different capacities on this engagement. His most recent role on the project was of working as a Project Manager at the client site in Boston, MA. He was responsible for overseeing day to day functioning of a 20-member team responsible for maintaining UI Online application.

- Responsible for the day to day functioning of the project
- Manage a team of 20 Deloitte practitioners working side by side with a bigger client team
- Manage system enhancement initiatives through each phase of SDLC phases
- Manage ongoing maintenance releases of the system
- Prepare status reports to multiple levels of higher management
- Work with client Project Manager, Agency Director, and other executives to identify risks, propose mitigation plan and provide status for executive consumption.

Technical Environment: .Net, Oracle, IBM FileNet, Team Foundation Server.

Project: The Pennsylvania Liquor Control Board (PLCB) iPhone app

Role: Application Manager; 4 months.

Limited by a state-restricted number of brick and mortar stores, the PLCB turned to Deloitte for a creative solution to upgrade and expand its retail operation. Deloitte team was tasked with conceiving, designing, developing and releasing the mobile iPhone app. For the first time ever, Pennsylvania consumers can browse products, compare prices, read reviews, and "click-to-buy" wine and spirits from anywhere in the Commonwealth. On-the-go customers can locate stores, verify inventory, and access real-time information about special discounts and promotions.

Responsibilities: As an Application Manager, Lenin was responsible for managing a team of high performing resources engaged in a cutting-edge space of mobile application development. His primary responsibilities involved working with the client to identify requirements, assess feasibility of implementing these requirements on mobile platform, planning development through release phases and monitoring progress.

- Responsible for the requirements validation, general system analysis and design
- Led and facilitated JAD sessions (Joint Application Development) with the client to validate the requirement and propose solutions
- Prioritized different business areas, client communication, and establishing work priorities
- Provided project status reports and business metrics on a regular basis
- Responsible for the day to day functioning of a high performing team using cutting edge technology and tools to design and develop mobile application
- Manage various testing phases, app release in Apple app store, post go-live maintenance and operations through issue resolution and subsequent app releases to support better business and technical functionalities

Technical Environment: XCode, JIRA, Various Supply Chain Management Platform

Project: The Alabama Department of Human Resources (DHR)

Role: Technical Manager; 24 months.

Deloitte implemented "Family, Adult and Child Tracking System" (Alabama FACTS) that provides DHR a comprehensive, integrated automated information system that is worker-driven, but also capable of capturing management information needs. The system captures, monitors, and accounts for all factors of

Deloitte

social services including: Foster care and adoption services; Child and adult protection and out-of-home care; Family preservation and support services and Independent living services.

Responsibilities: As Technical Manager Lenin was responsible for helping to confirm the integration of all technical aspects of Alabama FACTS project. As a key member of the project management team, he managed technical activities, addressed issues and communicated any potential risks to his project management colleagues.

- Evaluate, develop, configure and deploy infrastructure specifications;
- Manage application development team, overall implementation and training;
- Lead common service and component development;
- Manage Load and Performance testing activities using Visual Studio Team Suite (VSTS);
- Author client deliverables;
- Manage third party vendor relationships (IBM, Netrics, SKELTA etc)
- Manage data conversion from legacy to the new system, disaster recovery plan, pilot go-live in multiple counties, post go-live support through incident management

Technical Environment: .Net, IBM DB2, Netrics, Visual Source Safe.

Project: The District of Columbia Child and Family Services Agency (CDSA)

Role: Development Manager; 39 months.

Deloitte designed and implemented Statewide Automated Child Welfare System using ASP.Net / Oracle. The system supports social workers and the Agency in providing critical services related to case management activities such as writing case plans, documenting visits and writing court reports; standardizing policy and practice; collecting data to produce outcome-based management and issuing payment to service providers. Subsequently Deloitte was awarded contract to maintain and operate this state of the art web application.

Responsibilities: As an Offshore Project Manager, Lenin was responsible for overseeing day to day functioning of a 10-member team responsible for maintaining FACES.Net application. His primary responsibility involved working with the client to identify and triage defects, help prioritize them and ensure their on-time delivery. His job profile also involved travelling to Washington DC to work with the client for gathering new requirements, scoping and planning the delivery of these requirements in the form of technical solution.

- Responsible for the day to day functioning of the project
- Manage a team of 10 off-shore resources
- Manage system enhancement initiatives through each phase of SDLC phases
- Manage ongoing maintenance releases of the system
- Develop and maintain strategic client relationships
- Help track Project Risks and Issues
- Prepare status reports to multiple levels of higher management
- Manage priorities between different business areas involved client communication, establishing work priorities, and discussing business requirements
- Help manage the budgeting and staffing of the project

Technical Environment: .Net, Oracle, Visual Studio Team Foundation Server.

Previous Experience

Deloitte

Project: Multiple projects while working for Deloitte, Accenture, Thomson Financial

Role: Developer / Technical lead; 42 months.

Lenin worked on multiple projects to design, develop and implement custom developed systems primarily using various Microsoft technologies. He worked with multiple clients including Revenue & Tax Department of Singapore, Thomson Financials, and SPAR INC.

Responsibilities: Lenin worked as a .Net developer.

- Understanding Functional Specifications;
- Configuration Management through automation of build and deployment process using NANTS;
- Fine tuning application for enhancing the Developing ASP.Net components, user controls, custom controls and Oracle Package;
- Integrating various components into deliverable units.

Technical Environment: .Net, Oracle, Visual Studio.

Education

Master of Computer Application

University of Mumbai

Bachelor of Commerce

University of Mumbai



Aswin Kathirasetty

Summary of Experience and Qualifications

Aswin Kathirasetty is a seasoned application optimization specialist with over 14 years of experience in performance planning, testing, optimizing applications and applying enterprise architecture principles across different platforms. He possesses very good experience on Microsoft server technologies like ASP.NET, BizTalk, and SQL server to name a few. He has experience in tuning systems built out of Java on Linux platforms as well. He is very methodical and creative and has solved very many problems for huge state sector projects.

He is go-to person across multiple west coast public sector projects for application optimization within Deloitte, with the ability to identify and resolve complex scalability/performance issues within large scale custom implementations.

Deloitte Experience

Industry: Public Sector

Offering Portfolio: Health Technology

Competency Area: Performance Optimization and System Architecture

Duration: 3 Years 5 months.

California Department of Health

Role: Managed performance testing and optimization activities across multiple CDPH projects. In last few years within CDPH, I have tested and optimized Genetic Disease Screening Program (GDSP) application post data center migration, Medical Cannabis Licensing (MCLS), Office of Aids ADAP Enrollment, Vital Statistics Query 2 and L&C systems.

Worked with functional teams to understand the business requirements to help design and develop load scenarios. Developed automation scripts using LoadRunner, executed load tests using load controller and agents. Monitored load tests to identify bottlenecks within applications and infrastructure configuration using SCOM, AVICODE Profiler and SQL DMV's. In case of issues with application code, performed thread and memory dump analysis using Microsoft Debugging Toolkit to identify performance hotspots in code. Provided recommendations to development and infrastructure teams to fix issues within application code and infrastructure configuration.

Managed Architecture Review Board (ARB) within GDSP to make sure that the enhancements and changes performed on GDSP SIS solution are scalable and meets all performance service level agreements.

Industry: Public Sector

Offering Portfolio: Health Technology

Competency Area: Performance Optimization and System Architecture

Duration: 2 Years 5 months.

Washington Paid Family leave

Role: Managed performance testing and optimization activities for Washington PFML project. Worked with functional teams to understand the business requirements to help design and develop load scenarios. Developed automation scripts using visual studio load test services, executed load tests using Azure cloud load agents. Monitored load tests using Application Insight, MS SQL Query Store and Perfmon to identify bottlenecks within applications and infrastructure configuration. In case of issues with application code, performed thread and memory dump analysis using Microsoft Debugging Toolkit to identify performance hotspots in code. Provided recommendations to development and infrastructure teams to fix issues within application code and infrastructure configuration.

As part of this project, I have also developed a performance testing framework using C# to develop automation scripts and maintain data.

Industry: Public Sector**Offering Portfolio: Health Technology****Competency Area: Performance Optimization and System Architecture****Duration: 10 Years 2 months.**

Employment Development Department

Role: Managed performance testing and optimization activities for EDD Disability Insurance and Unemployment Insurance applications after integrating with Oracle 11G identity management system. Worked with functional teams to understand the business requirements to help design and develop load scenarios. Developed automation scripts using Performance Center, executed load tests using load controller and agents. Monitored load tests to identify bottlenecks within applications and infrastructure configuration using SCOM and SiteScope. In case of issues with application code, performed thread and memory dump analysis using Microsoft Debugging Toolkit to identify performance hotspots in code. Provided recommendations to development and infrastructure teams to fix issues within application code and infrastructure configuration.

Managed performance testing and optimization activities for EDD Disability Insurance and Unemployment Insurance applications. Worked with functional teams to understand the business requirements to help design and develop load scenarios. Developed automation scripts using performance center, executed load tests using load controller and agents. Monitored load tests to identify bottlenecks within applications and infrastructure configuration using SCOM and SiteScope. Provided recommendations to fix issues within application code and infrastructure configuration.

Industry: Public Sector**Offering Portfolio: Health Technology****Competency Area: Performance Optimization and System Architecture****Duration: 10 Years 2 months.**

Oregon Medicaid

Role: Managed performance testing and optimization activities for Oregon MAGI Medicaid solution. Worked with functional teams to understand the business requirements to help design and develop load scenarios. Developed automation scripts using Visual Studio, executed load tests using visual studio load controller and agents. Monitored load tests to identify bottlenecks within applications and infrastructure configuration using SCOM. Provided recommendations to fix issues within application code and infrastructure configuration.

Previous Experience

Industry: Private Sector

Competency Area: Performance Optimization and System Architecture

Duration: 1 Years 6 months.

Sempra Utilities\Aryasai inc

Role: Worked with functional teams to understand the business requirements to help design and develop load scenarios. Developed automation scripts using performance center, executed load tests using load controller and agents. Monitored load tests to identify bottlenecks within applications and infrastructure configuration. Provided recommendations to fix issues within application code and infrastructure configuration.

Industry: Private Sector

Competency Area: Performance Optimization and System Architecture

Duration: 9 months.

EMC

Role: Worked with functional teams to understand the business requirements to help design and develop load scenarios. Developed automation scripts using performance center, executed load tests using load controller and agents. Monitored load tests to identify bottlenecks within applications and infrastructure configuration. Provided recommendations to fix issues within application code and infrastructure configuration.

System Experience

Software / Products: Loadrunner, Performance Center, Jmeter, Visual Studio Load Test, Systems Center Operations Monitoring (SCOM), SiteScope, SQL Server, Biztalk, Avicode, In Rule Rules Engine, PARASCIPT iOCR, Azure DevOps

Development Tools / Languages: C, C#, Power Shell Scripting, Visual Studio, PLSQL

Hardware / Operating Systems: All Enterprise Windows Servers

Middleware / Databases: Biztalk Service Bus, Azure Service Bus, SQL Server 2008, 2012 and 2016

General Tools: Microsoft Excel, Microsoft Word, Microsoft Power Point, Microsoft Project, Visio

Education

Masters in Software Engineering

San Jose State University

Bachelors in Computer Science

Visveswaraya Technology University (Belgaum, Karnataka, india)

**ATTACHMENT 5
FEMA PROVISIONS**

1. EQUAL EMPLOYMENT OPPORTUNITY

During the performance of this contract, the contractor agrees as follows:

- A. The contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following:

Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.

- B. The contractor will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.
- C. The contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the contractor's legal duty to furnish information.
- D. The contractor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice to be provided advising the said labor union or workers' representatives of the contractor's commitments under this section, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.
- E. The contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.
- F. The contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.
- G. In the event of the contractor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this contract may be canceled, terminated, or suspended in whole or in part and the contractor may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.
- H. The contractor will include the portion of the sentence immediately preceding paragraph (1) and the provisions of paragraphs (1) through (8) in every subcontract or purchase order unless exempted by rules,

regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance:

Provided, however, that in the event a contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the administering agency, the contractor may request the United States to enter into such litigation to protect the interests of the United States.

The applicant further agrees that it will be bound by the above equal opportunity clause with respect to its own employment practices when it participates in federally assisted construction work: Provided, That if the applicant so participating is a State or local government, the above equal opportunity clause is not applicable to any agency, instrumentality or subdivision of such government which does not participate in work on or under the contract.

The applicant agrees that it will assist and cooperate actively with the administering agency and the Secretary of Labor in obtaining the

compliance of contractors and subcontractors with the equal opportunity clause and the rules, regulations, and relevant orders of the Secretary of Labor, that it will furnish the administering agency and the Secretary of Labor such information as they may require for the supervision of such compliance, and that it will otherwise assist the administering agency in the discharge of the agency's primary responsibility for securing compliance.

The applicant further agrees that it will refrain from entering into any contract or contract modification subject to Executive Order 11246 of September 24, 1965, with a contractor debarred from, or who has not demonstrated eligibility for, Government contracts and federally assisted construction contracts pursuant to the Executive Order and will carry out such sanctions and penalties for violation of the equal opportunity clause as may be imposed upon

2. CONTRACT WORK HOURS AND SAFETY STANDARDS ACT

Compliance with the Contract Work Hours and Safety Standards Act.

- A. ***Overtime requirements.*** No contractor or subcontractor contracting for any part of the contract work which may require or involve the employment of laborers or mechanics shall require or permit any such laborer or mechanic in any workweek in which he or she is employed on such work to work in excess of forty hours in such workweek unless such laborer or mechanic receives compensation at a rate not less than one and one-half times the basic rate of pay for all hours worked in excess of forty hours in such workweek.
- B. ***Violation; liability for unpaid wages; liquidated damages.*** In the event of any violation of the clause set forth in paragraph (b)(1) of this section the contractor and any subcontractor responsible therefor shall be liable for the unpaid wages. In addition, such contractor and subcontractor shall be liable to the United States (in the case of work done under contract for the District of Columbia or a territory, to such District or to such territory), for liquidated damages. Such liquidated damages shall be computed with respect to each individual laborer or mechanic, including watchmen and guards, employed in violation of the clause set forth in paragraph (b)(1) of this section, in the sum of \$27 for each calendar day on which such individual was required or permitted to work in excess of the standard workweek of forty hours without payment of the overtime wages required by the clause set forth in paragraph (b)(1) of this section.
- C. ***Withholding for unpaid wages and liquidated damages.*** The State of California shall upon its own action or upon written request of an authorized representative of the Department of Labor withhold or cause to be withheld, from any moneys payable on account of work performed by the contractor or subcontractor under any such contract or any other Federal contract with the same prime contractor, or any other federally-assisted contract subject to the Contract Work Hours and Safety Standards Act, which is held by the same prime contractor, such sums as may be determined to be necessary to satisfy any liabilities of such contractor

or subcontractor for unpaid wages and liquidated damages as provided in the clause set forth in paragraph (b)(2) of this section.

- D. ***Subcontracts.*** The contractor or subcontractor shall insert in any subcontracts the clauses set forth in paragraph (b)(1) through (4) of this section and also a clause requiring the subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for compliance by any subcontractor or lower tier subcontractor with the clauses set forth in paragraphs (b)(1) through (4) of this section.

3. CLEAN AIR ACT

- A. The contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. Section 7401 et seq.
- B. The contractor agrees to report each violation to the California Air Resources Board and understands and agrees that the California Air Resources Board will, in turn, report each violation as required to assure notification to the Department of Resources Recycling and Recovery, the California Governor's Office of Emergency Services, Federal Emergency Management Agency (FEMA), and the appropriate Environmental Protection Agency Regional Office.
- C. The contractor agrees to include these requirements in each subcontract exceeding \$150,000 financed in whole or in part with Federal assistance provided by FEMA.

4. THE FEDERAL WATER POLLUTION CONTROL ACT

- A. The contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. Sections 1251 et seq.
- B. The contractor agrees to report each violation to the State Water Resources Control Board and understands and agrees that the State Water Resources Control Board will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency (FEMA), and the appropriate Environmental Protection Agency Regional Office.
- C. The contractor agrees to include these requirements in each subcontract exceeding \$150,000 financed in whole or in part with Federal assistance provided by FEMA.

5. DEBARMENT AND SUSPENSION CLAUSE

- A. This contract is a covered transaction for purposes of 2 C.F.R. pt. 180 and 2 C.F.R. pt. 3000. As such the contractor is required to verify that none of the contractor, its principals (defined at 2 C.F.R. § 180.995), or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935).
- B. The contractor must comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.
- C. This certification is a material representation of fact relied upon by the State of California. If it is later determined that the contractor did not comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, in addition to remedies available to the State of California, the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.
- D. The bidder proposer agrees to comply with the requirements of 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. The bidder or proposer further agrees to include a provision requiring such compliance in its lower tier covered transactions.

6. BYRD ANTI-LOBBYING CLAUSE

Byrd Anti-Lobbying Amendment, 31 U.S.C. § 1352 (as amended). Contractors who apply or bid for an award of \$100,000 or more shall file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Each tier shall also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the recipient.

APPENDIX A. 44 C.F.R. PART 18- CERTIFICATION REGARDING LOBBYING

The undersigned [Contractor] certifies, to the best of his or her knowledge, that:

- A. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.
- B. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form- LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.
- C. The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by 31, U.S.C. § 1352 (as amended by the Lobbying Disclosure Act of 1995). Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

The Contractor certifies or affirms the truthfulness and accuracy of each statement of its certification and disclosure, if any. In addition, the Contractor understands and agrees that the provisions of 31 U.S.C. § 3801 et seq., apply to this certification and disclosure, if any.

Signature of Contractor's Authorized Official

Name and Title of Contractor's Authorized Official

Date:

7. PROCUREMENT OF RECOVERED MATERIALS

- A. In the performance of this contract the Contractor shall make maximum use of products containing recovered materials that are EPA- designated items unless the product cannot be acquired:
 - i. Competitively within a timeframe providing for compliance with the contract performance schedule;
 - ii. Meeting contract performance requirements; or
 - iii. At a reasonable price.
- B. Information about this requirement is available at EPA's Comprehensive Procurement Guidelines web site, <http://www.epa.gov/cpg/>. The list of EPA-designate items is available at <https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program>.
- C. The Contractor also agrees to comply with all other applicable requirements of Section 6002 of the Solid Waste Disposal Act.

8. ACCESS TO RECORDS

The following access to records requirements apply to this contract:

- A. The Contractor agrees to provide the State of California, the FEMA Administrator, the Controller General of the United States, or any of their authorized representatives access to any books, documents, papers, and records of the Contractor which are directly pertinent to this contract for the purposes of making audits, examinations, excerpts, and transcriptions.
- B. The Contractor agrees to permit any of the foregoing parties to reproduce by any means whatsoever of to copy excerpts and transcriptions as reasonably needed.
- C. The contractor agrees to provide the FEMA Administrator or his authorized representative access to construction or other work sites pertaining to the work being completed under the contract.
- D. In compliance with the Disaster Recovery Act of 2018, the State of California and the Contractor acknowledge and agree that no language in this contract is intended to prohibit audits or internal reviews by the FEMA Administrator or the Comptroller General of the United States.

9. DHS SEAL, LOGO, AND FLAGS

The contractor shall not use the DHS seal(s), logos, crests, or reproductions of flags or likenesses of DHS agency officials without specific FEMA pre-approval.

10. COMPLIANCE WITH FEDERAL LAW, REGULATIONS, AND EXECUTIVE ORDERS

This is an acknowledgement that FEMA financial assistance will be used to fund all or a portion of the contract only. The contractor will comply with all federal law, regulations, executive orders, FEMA policies, procedures, and directives.

11. NO OBLIGATION BY FEDERAL GOVERNMENT

The Federal Government is not a party to this contract and is not subject to any obligations or liabilities to the non-Federal entity, contractor, or any other party pertaining to any matter resulting from the contract.

12. PROGRAM FRAUD AND FALSE OR FRAUDULENT STATEMENTS OR RELATED ACTS

The contractor acknowledges the 31 U.S.C. Chapter 38 (Administrative Remedies for False Claims and Statements) applies to the contractor's action pertaining to this contract.

Attachment 5
Contractor's Release

Instructions to Contractor:

With final invoice(s) submit one (1) original and one (1) copy. The original must bear the original signature of a person authorized to bind the Contractor. The additional copy may bear photocopied signatures.

Submission of Final Invoice

Pursuant to contract number 21-10459 entered into between the State of California Department of Public Health (CDPH) and the Contractor (identified below), the Contractor does acknowledge that final payment has been requested via invoice number(s) _____, in the amount(s) of \$ _____ and dated _____

If necessary, enter "See Attached" in the appropriate blocks and attach a list of invoice numbers, dollar amounts and invoice dates.

Release of all Obligations

By signing this form, and upon receipt of the amount specified in the invoice number(s) referenced above, the Contractor does hereby release and discharge the State, its officers, agents and employees of and from any and all liabilities, obligations, claims, and demands whatsoever arising from the above referenced contract.

Repayments Due to Audit Exceptions / Record Retention

By signing this form, Contractor acknowledges that expenses authorized for reimbursement does not guarantee final allowability of said expenses. Contractor agrees that the amount of any sustained audit exceptions resulting from any subsequent audit made after final payment will be refunded to the State.

All expense and accounting records related to the above referenced contract must be maintained for audit purposes for no less than three years beyond the date of final payment, unless a longer term is stated in said contract.

Recycled Product Use Certification

By signing this form, Contractor certifies under penalty of perjury that a minimum of 0% unless otherwise specified in writing of post consumer material, as defined in the Public Contract Code Section 12200, in products, materials, goods, or supplies offered or sold to the State regardless of whether it meets the requirements of Public Contract Code Section 12209. Contractor specifies that printer or duplication cartridges offered or sold to the State comply with the requirements of Section 12156(e).

Reminder to Return State Equipment/Property (If Applicable)

(Applies only if equipment was provided by CDPH or purchased with or reimbursed by contract funds)

Unless CDPH has approved the continued use and possession of State equipment (as defined in the above referenced contract) for use in connection with another CDPH agreement, Contractor agrees to promptly initiate arrangements to account for and return said equipment to CDPH, at CDPH's expense, if said equipment has not passed its useful life expectancy as defined in the above referenced contract.

Patents / Other Issues

By signing this form, Contractor further agrees, in connection with patent matters and with any claims that are not specifically released as set forth above, that it will comply with all of the provisions contained in the above referenced contract, including, but not limited to, those provisions relating to notification to the State and related to the defense or prosecution of litigation.

ONLY SIGN AND DATE THIS DOCUMENT WHEN ATTACHING TO THE FINAL INVOICE

Contractor's Legal Name (as on contract): Deloitte Consulting LLP

Signature of Contractor or Official Designee: _____ Date: _____

Printed Name/Title of Person Signing: _____

CDPH Distribution: Accounting (Original) Program

ATTACHMENT 7
HIPAA Business Associate Addendum

I. Recitals

- A. The underlying contract (Agreement), to which this HIPAA Business Associate Addendum is attached to and made a part of, has been determined to constitute a business associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), 42 U.S.C. section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations").
- B. The Department of Public Health ("CDPH") wishes to disclose to Business Associate certain information pursuant to the terms of the Agreement, some of which may constitute Protected Health Information ("PHI"), including protected health information in electronic media ("ePHI"), under federal law, and personal information ("PI") under state law.
- C. As set forth in the Agreement, Contractor, here and after, is the Business Associate of CDPH acting on CDPH' behalf and provides services, arranges, performs or assists in the performance of functions or activities on behalf of CDPH and creates, receives, maintains, transmits, uses or discloses PHI and PI. CDPH and Business Associate are each a party to the Agreement and are collectively referred to as the "parties."
- D. The purpose of this Addendum is to protect the privacy and security of the PHI and PI that may be created, received, maintained, transmitted, used or disclosed pursuant to the Agreement, and to comply with certain standards and requirements of HIPAA, the HITECH Act and the HIPAA regulations, including, but not limited to, the requirement that CDPH must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 CFR Parts 160 and 164 and the HITECH Act.
- E. The terms used in this Addendum, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

II. Definitions

- A. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- B. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- C. Covered Entity shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- D. Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C Section 17921 and implementing regulations.
- E. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 CFR section 160.103.

- F. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 CFR section 160.103.
- G. Privacy Rule shall mean the HIPAA Regulation that is found at 45 CFR Parts 160 and 164.
- H. Personal Information shall have the meaning given to such term in California Civil Code sections 1798.3 and 1798.29..
- I. Protected Health Information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR section 160.103.
- J. Required by law, as set forth under 45 CFR section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
- K. Secretary means the Secretary of the U.S. Department of Health and Human Services ("HHS") or the Secretary's designee.
- L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or PI, or confidential data that is essential to the ongoing operation of the Business Associate's organization and intended for internal use; or interference with system operations in an information system.
- M. Security Rule shall mean the HIPAA regulation that is found at 45 CFR Parts 160 and 164.
- N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. section 17932(h), any guidance issued pursuant to such Act and the HIPAA regulations.

III. Terms of Agreement

A. Permitted Uses and Disclosures of PHI by Business Associate

Permitted Uses and Disclosures. Except as otherwise indicated in this Addendum, Business Associate may use or disclose PHI only to perform functions, activities or services specified in the Agreement, for, or on behalf of CDPH, provided that such use or disclosure would not violate the HIPAA regulations, if done by CDPH. Any such use or disclosure must, to the extent practicable, be limited to the limited data set, as defined in 45 CFR section 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, and the HIPAA regulations.

1. **Specific Use and Disclosure Provisions.** Except as otherwise indicated in this Addendum, Business Associate may:

- a. ***Use and disclose for management and administration.*** Use and disclose PHI for the proper management and administration of the Business Associate provided that such disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.
- b. ***Provision of Data Aggregation Services.*** Use PHI to provide data aggregation services to CDPH. Data aggregation means the combining of PHI created or received by the Business Associate on behalf of CDPH with PHI received by the Business Associate in its capacity as the Business Associate of another covered entity, to permit data analyses that relate to the health care operations of CDPH.

B. Prohibited Uses and Disclosures

1. Business Associate shall not disclose PHI about an individual to a health plan for payment or health care operations purposes if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. section 17935(a) and 45 CFR section 164.522(a).
2. Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of CDPH and as permitted by 42 U.S.C. section 17935(d)(2).

C. Responsibilities of Business Associate

Business Associate agrees:

1. ***Nondisclosure.*** Not to use or disclose Protected Health Information (PHI) other than as permitted or required by the Agreement or as required by law.
2. ***Safeguards.*** To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of CDPH, in compliance with 45 CFR sections 164.308, 164.310 and 164.312, and to prevent use or disclosure of PHI other than as provided for by the Agreement. Business Associate shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR section 164, subpart C, in compliance with 45 CFR section 164.316. Business Associate shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Business Associate's operations and the nature and scope of its activities, and which incorporates the requirements of section 3, Security, below. Business Associate will provide CDPH with its current and updated policies.
3. ***Security.*** To take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:
 - a. Complying with all of the data system security precautions listed in Attachment A, the Business Associate Data Security Requirements;

- b. Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of CDPH under the Agreement;
- c. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and
- d. In case of a conflict between any of the security standards contained in any of these enumerated sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI from unauthorized disclosure. Further, Business Associate must comply with changes to these standards that occur after the effective date of the Agreement.
- e. Business Associate shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with CDPH.

D. Mitigation of Harmful Effects. To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or its subcontractors in violation of the requirements of this Addendum.

E. Business Associate's Agents and Subcontractors.

- 1. To enter into written agreements with any agents, including subcontractors and vendors, to whom Business Associate provides PHI or PI received from or created or received by Business Associate on behalf of CDPH, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Business Associate with respect to such PHI and PI under this Addendum, and that comply with all applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations.
- 2. In accordance with 45 CFR section 164.504(e)(1)(ii), upon Business Associate's knowledge of a material breach or violation by its subcontractor of the agreement between Business Associate and the subcontractor, Business Associate shall:
 - a. Provide an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by CDPH; or
 - b. Immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.

F. Availability of Information to CDPH and Individuals. To provide access and information:

- 1. To provide access as CDPH may require, and in the time and manner designated by CDPH (upon reasonable notice and during Business Associate's normal business hours) to PHI in a Designated Record Set, to CDPH (or, as directed by CDPH), to an Individual, in accordance with 45 CFR section 164.524. Designated Record Set means the group of records maintained for CDPH that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for CDPH health plans; or those records used to make decisions about individuals on behalf of CDPH. Business Associate shall use the forms and processes developed by CDPH for this purpose and shall respond to requests for access to records

transmitted by CDPH within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.

2. If Business Associate maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Business Associate shall provide such information in an electronic format to enable CDPH to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. section 17935(e).
3. If Business Associate receives data from CDPH that was provided to CDPH by the Social Security Administration, upon request by CDPH, Business Associate shall provide CDPH with a list of all employees, contractors and agents who have access to the Social Security data, including employees, contractors and agents of its subcontractors and agents.

G. Amendment of PHI. To make any amendment(s) to PHI that CDPH directs or agrees to pursuant to 45 CFR section 164.526, in the time and manner designated by CDPH.

H. Internal Practices. To make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from CDPH, or created or received by Business Associate on behalf of CDPH, available to CDPH or to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by CDPH or by the Secretary, for purposes of determining CDPH' compliance with the HIPAA regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Business Associate, Business Associate shall so certify to CDPH and shall set forth the efforts it made to obtain the information.

I. Documentation of Disclosures. To document and make available to CDPH or (at the direction of CDPH) to an Individual such disclosures of PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 CFR section 164.528 and 42 U.S.C. section 17935(c). If Business Associate maintains electronic health records for CDPH as of January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after January 1, 2014. If Business Associate acquires electronic health records for CDPH after January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after the date the electronic health record is acquired, or on or after January 1, 2011, whichever date is later. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting.

J. Breaches and Security Incidents. During the term of the Agreement, Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

1. **Notice to CDPH.** (1) To notify CDPH **immediately by telephone call plus email or fax** upon the discovery of a breach of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of a suspected security incident that involves data provided to CDPH by the Social Security Administration. (2) To notify CDPH **within 24 hours by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of the Agreement and this Addendum, or potential loss of confidential data affecting the Agreement. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any

person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.

Notice shall be provided to the CDPH Program Contract Manager, the CDPH Privacy Officer and the CDPH Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notice shall be provided by calling the CDPH ITSD Service Desk. Notice shall be made using the "CDPH Privacy Incident Report" form, including all information known at the time. Business Associate shall use the most current version of this form, which is posted on the CDPH Privacy Office website (www.CDPH.ca.gov,

Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI, Business Associate shall take:

- a. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
- b. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
2. **Investigation and Investigation Report.** To immediately investigate such security incident, breach, or unauthorized access, use or disclosure of PHI or PI. Within 72 hours of the discovery, Business Associate shall submit an updated "CDPH Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Information Security Officer;
3. **Complete Report.** To provide a complete report of the investigation to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "CDPH Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or state law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If CDPH requests information in addition to that listed on the "CDPH Privacy Incident Report" form, Business Associate shall make reasonable efforts to provide CDPH with such information. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "CDPH Privacy Incident Report" form. CDPH will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.
4. **Notification of Individuals.** If the cause of a breach of PHI or PI is attributable to Business Associate or its subcontractors, agents or vendors, Business Associate shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days. The CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Information Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.
5. **Responsibility for Reporting of Breaches.** If the cause of a breach of PHI or PI is attributable to Business Associate or its agents, subcontractors or vendors, Business Associate is responsible for

all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured PHI involves more than 500 residents of the State of California or its jurisdiction, Business Associate shall notify the Secretary of the breach immediately upon discovery of the breach. If Business Associate has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to CDPH in addition to Business Associate, Business Associate shall notify CDPH, and CDPH and Business Associate may take appropriate action to prevent duplicate reporting. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in subsection 1, above.

6. **CDPH Contact Information.** To direct communications to the above referenced CDPH staff, the Contractor shall initiate contact as indicated herein. CDPH reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

CDPH Program Contract Manager	CDPH Privacy Officer	CDPH Information Security Officer
See the Scope of Work exhibit for Program Contract Manager information	Privacy Officer Privacy Office, c/o Office of Legal Services California Department of Public Health 1415 L Street, 5 th Floor Sacramento, CA 95814 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	Chief Information Security Officer Information Security Office California Department of Public Health P.O. Box 997413, MS 6302 Sacramento, CA 95899-7413 Email: cdphiso@cdph.ca.gov Telephone: IT Service Desk (916) 440-7000 or (800) 579-0874

K. Termination of Agreement. In accordance with Section 13404(b) of the HITECH Act and to the extent required by the HIPAA regulations, if Business Associate knows of a material breach or violation by CDPH of this Addendum, it shall take the following steps:

1. Provide an opportunity for CDPH to cure the breach or end the violation and terminate the Agreement if CDPH does not cure the breach or end the violation within the time specified by Business Associate; or
2. Immediately terminate the Agreement if CDPH has breached a material term of the Addendum and cure is not possible.

L. Due Diligence. Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Addendum and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Addendum.

M. Sanctions and/or Penalties. Business Associate understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to Business Associate may result in the imposition of sanctions and/or penalties on Business Associate under HIPAA, the HITECH Act and the HIPAA regulations.

IV. Obligations of CDPH

CDPH agrees to:

- A. Notice of Privacy Practices.** Provide Business Associate with the Notice of Privacy Practices that CDPH produces in accordance with 45 CFR section 164.520, as well as any changes to such notice.
- B. Permission by Individuals for Use and Disclosure of PHI.** Provide the Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect the Business Associate's permitted or required uses and disclosures.
- C. Notification of Restrictions.** Notify the Business Associate of any restriction to the use or disclosure of PHI that CDPH has agreed to in accordance with 45 CFR section 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.
- D. Requests Conflicting with HIPAA Rules.** Not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA regulations if done by CDPH.

V. Audits, Inspection and Enforcement

- A.** From time to time, CDPH may inspect the facilities, systems, books and records of Business Associate to monitor compliance with the Agreement and this Addendum. Business Associate shall promptly remedy any violation of any provision of this Addendum and shall certify the same to the CDPH Privacy Officer in writing. The fact that CDPH inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Addendum, nor does CDPH:

1. Failure to detect or
 2. Detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of CDPH' enforcement rights under the Agreement and this Addendum.
- B.** If Business Associate is the subject of an audit, compliance review, or complaint investigation by the Secretary or the Office of Civil Rights, U.S. Department of Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Addendum, Business Associate shall notify CDPH and provide CDPH with a copy of any PHI or PI that Business Associate provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI or PI to the Secretary. Business Associate is responsible for any civil penalties assessed due to an audit or investigation of Business Associate, in accordance with 42 U.S.C. section 17934(c).

VI. Termination

- A. *Term.*** The Term of this Addendum shall commence as of the effective date of this Addendum and shall extend beyond the termination of the Agreement and shall terminate when all the PHI provided by CDPH to Business Associate, or created or received by Business Associate on behalf of CDPH, is destroyed or returned to CDPH, in accordance with 45 CFR 164.504(e)(2)(ii)(I).
- B. *Termination for Cause.*** In accordance with 45 CFR section 164.504(e)(1)(ii), upon CDPH' knowledge of a material breach or violation of this Addendum by Business Associate, CDPH shall:
1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Agreement if Business Associate does not cure the breach or end the violation within the time specified by CDPH; or
 2. Immediately terminate the Agreement if Business Associate has breached a material term of this Addendum and cure is not possible.
- C. *Judicial or Administrative Proceedings.*** Business Associate will notify CDPH if it is named as a defendant in a criminal proceeding for a violation of HIPAA. CDPH may terminate the Agreement if Business Associate is found guilty of a criminal violation of HIPAA. CDPH may terminate the Agreement if a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Business Associate is a party or has been joined.
- D. *Effect of Termination.*** Upon termination or expiration of the Agreement for any reason, Business Associate shall return or destroy all PHI received from CDPH (or created or received by Business Associate on behalf of CDPH) that Business Associate still maintains in any form, and shall retain no copies of such PHI. If return or destruction is not feasible, Business Associate shall notify CDPH of the conditions that make the return or destruction infeasible, and CDPH and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI. Business Associate shall continue to extend the protections of this Addendum to such PHI, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

VII. Miscellaneous Provisions

- A. *Disclaimer.*** CDPH makes no warranty or representation that compliance by Business Associate with this Addendum, HIPAA or the HIPAA regulations will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business

Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

- B. Amendment.** The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations and other applicable laws relating to the security or privacy of PHI. Upon CDPH's request, Business Associate agrees to promptly enter into negotiations with CDPH concerning an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations or other applicable laws. CDPH may terminate the Agreement upon thirty (30) days written notice in the event:
1. Business Associate does not promptly enter into negotiations to amend this Addendum when requested by CDPH pursuant to this Section; or
 2. Business Associate does not enter into an amendment providing assurances regarding the safeguarding of PHI that CDPH in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and the HIPAA regulations.
- C. Assistance in Litigation or Administrative Proceedings.** Business Associate shall make itself and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under the Agreement, available to CDPH at no cost to CDPH to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CDPH, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inactions or actions by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named adverse party.
- D. No Third-Party Beneficiaries.** Nothing express or implied in the terms and conditions of this Addendum is intended to confer, nor shall anything herein confer, upon any person other than CDPH or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.
- E. Interpretation.** The terms and conditions in this Addendum shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the HIPAA regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations.
- F. Regulatory References.** A reference in the terms and conditions of this Addendum to a section in the HIPAA regulations means the section as in effect or as amended.
- G. Survival.** The respective rights and obligations of Business Associate under Section VI.D of this Addendum shall survive the termination or expiration of the Agreement.
- H. No Waiver of Obligations.** No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

Attachment A
Business Associate Data Security Requirements

I. Personnel Controls

- A. Employee Training.** All workforce members who assist in the performance of functions or activities on behalf of CDPH, or access or disclose CDPH PHI or PI must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.
- B. Employee Discipline.** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
- C. Confidentiality Statement.** All persons that will be working with CDPH PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to CDPH PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for CDPH inspection for a period of six (6) years following contract termination.
- D. Background Check.** Before a member of the workforce may access CDPH PHI or PI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

II. Technical Security Controls

- A. Workstation/Laptop encryption.** All workstations and laptops that process and/or store CDPH PHI or PI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the CDPH Information Security Office.
- B. Server Security.** Servers containing unencrypted CDPH PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
- C. Minimum Necessary.** Only the minimum necessary amount of CDPH PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.
- D. Removable media devices.** All electronic files that contain CDPH PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.
- E. Antivirus software.** All workstations, laptops and other systems that process and/or store CDPH PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

- F. **Patch Management.** All workstations, laptops and other systems that process and/or store CDPH PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.
- G. **User IDs and Password Controls.** All users must be issued a unique user name for accessing CDPH PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:
- Upper case letters (A-Z)
 - Lower case letters (a-z)
 - Arabic numerals (0-9)
 - Non-alphanumeric characters (punctuation symbols)
- H. **Data Destruction.** When no longer needed, all CDPH PHI or PI must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the CDPH Information Security Office.
- I. **System Timeout.** The system providing access to CDPH PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.
- J. **Warning Banners.** All systems providing access to CDPH PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.
- K. **System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for CDPH PHI or PI, or which alters CDPH PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If CDPH PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.
- L. **Access Controls.** The system providing access to CDPH PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

- M. **Transmission encryption.** All data transmissions of CDPH PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.
- N. **Intrusion Detection.** All systems involved in accessing, holding, transporting, and protecting CDPH PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

III. Audit Controls

- A. **System Security Review.** All systems processing and/or storing CDPH PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.
- B. **Log Reviews.** All systems processing and/or storing CDPH PHI or PI must have a routine procedure in place to review system logs for unauthorized access.
- C. **Change Control.** All systems processing and/or storing CDPH PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

IV. Business Continuity / Disaster Recovery Controls

- A. **Emergency Mode Operation Plan.** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic CDPH PHI or PI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under the Agreement for more than 24 hours.
- B. **Data Backup Plan.** Contractor must have established documented procedures to backup CDPH PHI to maintain retrievable exact copies of CDPH PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore CDPH PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CDPH data.

V. Paper Document Controls

- A. **Supervision of Data.** CDPH PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. CDPH PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
- B. **Escorting Visitors.** Visitors to areas where CDPH PHI or PI is contained shall be escorted and CDPH PHI or PI shall be kept out of sight while visitors are in the area.
- C. **Confidential Destruction.** CDPH PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

- D. ***Removal of Data.*** CDPH PHI or PI must not be removed from the premises of the Contractor except with express written permission of CDPH.
- E. ***Faxing.*** Faxes containing CDPH PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.
- F. ***Mailing.*** Mailings of CDPH PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of CDPH PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of CDPH to use another method is obtained.



INFORMATION SECURITY OFFICE

Information Systems Security Requirements for Projects (ISO/SR1)

Version 4.0

February 2010

TABLE OF CONTENTS

I.	PURPOSE.....	4
II.	SCOPE OF REQUIREMENTS	4
III.	CONTACT.....	4
IV.	INFORMATION SYSTEMS SECURITY REQUIREMENTS.....	5
A.	ADMINISTRATIVE / MANAGEMENT SAFEGUARDS.....	5
1.	<i>Workforce Confidentiality Statement</i>	5
2.	<i>Access Authorization & Maintenance</i>	5
3.	<i>Information System Activity Review</i>	5
4.	<i>Periodic System Security & Log Review</i>	5
5.	<i>Disaster Recovery Plan</i>	6
6.	<i>Change Control</i>	6
7.	<i>Supervision of Information</i>	6
8.	<i>Escorting Visitors</i>	6
B.	TECHNICAL AND OPERATIONAL SAFEGUARDS.....	7
1.	<i>System Security Compliance</i>	7
2.	<i>Malware Protection</i>	7
3.	<i>Patch Management</i>	7
4.	<i>Encrypted Electronic Transmissions</i>	7
5.	<i>Encrypted Information Storage</i>	7
6.	<i>Workstation / Laptop Encryption</i>	7
7.	<i>Removable Media Encryption</i>	8
8.	<i>Secure Connectivity</i>	8
9.	<i>Intrusion Detection and Prevention</i>	8
10.	<i>Minimum Information Download</i>	8
11.	<i>Information Sanitization</i>	8
12.	<i>Removal of Information</i>	8
13.	<i>Faxing or Mailing of Information</i>	9
C.	SOLUTION ARCHITECTURE	10
1.	<i>System Security Compliance</i>	10
2.	<i>Warning Banner</i>	10
3.	<i>Layered Application Design</i>	10
4.	<i>Input Validation</i>	11
5.	<i>Data Queries</i>	11
6.	<i>Username/Password Based Authentication</i>	12
7.	<i>Administrative / Privileged Accounts Management</i>	12
8.	<i>Service Accounts Management</i>	13
9.	<i>Authentication and Authorization</i>	13
10.	<i>Authentication Logging</i>	14
11.	<i>Automatic System Session Expiration</i>	14
12.	<i>Automatic System Lock-out and Reporting</i>	14
13.	<i>Audit (Access)</i>	14
14.	<i>Audit (Minimum Information)</i>	14
15.	<i>Application Security Controls</i>	15
16.	<i>Application Code Security</i>	15
17.	<i>Strong Authentication</i>	16
D.	DOCUMENTATION OF SOLUTION	17
1.	<i>System Configuration</i>	17
2.	<i>Information Classification</i>	17
3.	<i>System Roles and Relationships</i>	17
4.	<i>Audit Method Documentation</i>	17
5.	<i>Retention of Documentation</i>	17
E.	ISO NOTIFICATIONS AND APPROVALS.....	18

1.	<i>Security Compliance Notification</i>	18
2.	<i>Notification of Changes to Solution</i>	18
3.	<i>Notification of Breach</i>	18
4.	<i>Project Security Approvals</i>	18
5.	<i>Application Security Approvals</i>	19
F.	APPENDIX A – SR1 EXEMPTION FORM	20



Type: ISO Requirements	
Issued: February 08, 2010	Doc Number: SR1 v4.0
Revised:	
Title: Information Systems Security Requirements for Projects	

IMPORTANT NOTE: If an exemption from any SR1 requirement is required, the SR1 Exemption Form in Appendix A must be completed by the Project Manager or Contract Manager.

I. Purpose

This document provides the minimum security requirements mandated by the California Department of Public Health (CDPH) Information Security Office (ISO) for projects governed and/or subject to the policies and standards of CDPH. Projects that intend to deploy systems/applications into the CDPH system infrastructure, or will utilize CDPH information system services, are also subject to these minimum security requirements.

This document is intended to assist CDPH and its service customers in understanding the criteria CDPH will use when evaluating and certifying the system design, security features and protocols used by project solutions utilizing CDPH services. These security requirements will also be used in conjunction with the CDPH ISO compliance review program of its information system services customers.

This document will serve as a universal set of requirements which must be met regardless of physical hosting location or entities providing operations and maintenance responsibility. These requirements do not serve any specific project, nor do they prescribe any specific implementation technology.

II. Scope of Requirements

The information security requirements in this document are organized in five categories (sections) and address at a minimum:

- Administrative/Management Safeguards
- Technical and Operational Safeguards
- Solution Architecture
- Documentation of Solution
- ISO Notifications and Approvals

III. Contact

Chief Information Security Officer
California Department of Public Health
Information Security Office (ISO)
cdphiso@cdph.ca.gov

IV. Information Systems Security Requirements

A. Administrative / Management Safeguards

1. Workforce Confidentiality Statement

All persons working with CDPH information must sign a Security and Confidentiality Acknowledgement Statement. The Statement must include, at a minimum: General Use, Security and Privacy safeguards, Unacceptable Use, Audit and Enforcement policies. (Contact the CDPH ISO for the current version of the Security & Confidentiality Acknowledgement Statement in use.)

The Statement must be signed by the Project member prior to being granted access to the CDPH information. The Statement must be renewed annually.

2. Access Authorization & Maintenance

Project/Program must document and implement clearly defined rules and processes for vetting and granting authorizations, as well as procedures for the supervision of workforce members who work with CDPH information or in locations where it might be accessed.

On at least a semi-annual basis, Project/Program will review and remove all authorizations for individuals who have left the department, transferred to another unit, or assumed new job duties within CDPH.

3. Information System Activity Review

Project/Program must implement and document procedures to regularly review records of information system activity (such as audit logs, access reports, and security incident tracking reports).

Project/Program must ensure any hosting or maintenance agreements clearly identify responsibility for this activity. Logs may be stored within the system or preferably on a centralized logging server or service, and must be maintained for a minimum of three years.

4. Periodic System Security & Log Review

All systems must allow for periodic system security reviews that provide assurance that management, operations, personnel, and technical controls are functioning effectively and providing adequate levels of protection.

These reviews may include technical tools and security procedures (such as vulnerability assessment products and penetration testing).

All systems processing and/or storing CDPH information must have a method or procedure in place to create and review system logs for unauthorized access. Logs may be stored within the system or on a centralized logging server or service, and must be maintained for a minimum of three years.

5. Disaster Recovery Plan

Project/Program will establish procedures that allow facility access in support of restoration of lost information under the Disaster Recovery Plan (DRP) and emergency mode operations plan in the event of an emergency.

The restoration/recovery support procedures must be added to the existing DRP to restore any loss of information and assure continuity of computing operations for support of both the application and information.

Recovery procedures must be developed using the most current DRP template provided by the CDPH ISO.

All systems, as part of a new or existing project, must allow for periodic system recovery testing. The period between tests should be defined as part of the project and be consistent with relevant CDPH disaster recovery standards. Such testing should provide assurances that plans and controls (management, operations, personnel, and technical) are functioning effectively and providing adequate levels of protection during an incident, disaster, or breach.

Project/Program will conduct an annual Business Impact Analysis of the application to determine the Maximum Acceptable Outage (MAO), cost of lost functionality, system component dependencies, business function dependencies, and business partner dependencies.

6. Change Control

All systems processing and/or storing CDPH information must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity, and availability of information.

Systems running within the CDPH environment and/or utilizing CDPH services must comply with CDPH standards for change control process and procedures.

7. Supervision of Information

Classified information in paper form must not be left unattended at any time, unless it is locked in a file cabinet, file room, desk, or office. Unattended means that information is not being observed by an employee authorized to access the information. Classified information in paper form must also not be left unattended at any time in vehicles or planes, and must not be transported in checked-in baggage on commercial airplanes.

8. Escorting Visitors

Visitors to areas where classified information is contained must be escorted and classified information must be kept out of sight while visitors are in the area.

B. Technical and Operational Safeguards

1. System Security Compliance

All Project systems must comply with applicable CDPH security policies and requirements, as specified in the State Administrative Manual (SAM), Public Health Administrative Manual (PHAM), Privacy Act, and any other applicable State or Federal regulation. All security safeguards and precautions must be subject to the approval of the CDPH ISO.

2. Malware Protection

All systems must install and actively use anti-virus software, with a minimum daily automatic update scheduled. Systems such as mainframes, where anti-virus is unavailable, are excluded from this requirement. All security safeguards and precautions must be subject to the approval of the CDPH ISO.

3. Patch Management

All systems must install and actively use a comprehensive third-party patch management program, and routinely update system and application software within two weeks of vendor release unless the CDPH ISO validates a patch is not applicable. Critical updates may require a more restrictive timeline. All security safeguards and precautions must be subject to the approval of the CDPH ISO.

4. Encrypted Electronic Transmissions

All information electronic transmissions that contain classified information (such as website access, file transfers or through e-mail) must be encrypted end-to-end using an industry-recognized encryption standard (such as Transport Layer Security (TLS) or its predecessor, Secure Socket Layer (SSL), Secure File Transfer Protocol (SFTP), or any FIPS 140-2 certified encryption algorithm). Classified information must be encrypted at the minimum of Advanced Encryption Standard (AES) with a 128 bit key or higher. Equivalent or stronger algorithms may be used upon approval of the CDPH ISO.

5. Encrypted Information Storage

All classified information must be encrypted when electronically stored using a CDPH approved encryption standard. Classified information must be encrypted at the minimum of AES with a 128 bit key or higher, or any FIPS 140-2 certified encryption algorithm. Equivalent or stronger algorithms may be used upon approval of the CDPH ISO.

6. Workstation / Laptop Encryption

All workstations and laptops that process and/or store classified CDPH information must be encrypted with a CDPH ISO approved solution. Classified CDPH information must be encrypted at the minimum of AES with a 128 bit key or higher, or any FIPS 140-2 certified encryption algorithm. Equivalent or stronger algorithms may be used upon approval of the CDPH ISO.

7. Removable Media Encryption

All electronic files that contain classified CDPH information must be encrypted at the minimum of AES with a 128 bit key or higher, or any FIPS 140-2 certified encryption algorithm when stored on any removable media type device (such as USB thumb drives, floppies, CD/DVD, tape backup, etc.). Equivalent or stronger algorithms may be used upon approval of the CDPH ISO. The solution should follow best practices described in National Institute of Standards & Technology (NIST) 800-111, Guide to Storage Encryption Technologies for End User Devices.

8. Secure Connectivity

All transmission and data-links between the information and application/system, and DBMS and the Office of Technology Services (OTech) Wide Area Network (WAN), must be secure between transmission systems as required by regulation, policy and/or standard and as prescribed for the given application/system.

9. Intrusion Detection and Prevention

All systems that are accessible via the Internet, are critical, and/or contain classified information must install and actively use a CDPH ISO approved comprehensive third-party real-time intrusion detection and prevention solution. The solution must also report security events directly to a CDPH enterprise monitoring solution. All security safeguards and precautions must be subject to the approval of the CDPH ISO.

10. Minimum Information Download

In accordance with the principle of need-to-know, only the minimum amount of information required to perform necessary business functions should be copied or downloaded.

11. Information Sanitization

All classified CDPH information (electronic or paper) must be sanitized from systems when the information is no longer necessary. The sanitization method must conform to NIST Special Publication 800-88 Guidelines for Media Sanitization. Once information has been sanitized, the CDPH contract manager must be notified. If an agency or other entity is unable to sanitize the media in accordance with NIST 800-88 and provide notification, the media must be returned to CDPH after usage for sanitization in an approved manner.

12. Removal of Information

Classified CDPH information (electronic or paper) must not be removed from CDPH premises, or from the premises of an authorized vendor or contractor, without the written permission of the CDPH ISO.

13. Faxing or Mailing of Information

Facsimile transmissions containing classified CDPH information must not be left unattended if fax machines are not in a secure area. Facsimile transmissions must include a cover sheet that contains a security statement notifying persons receiving faxes in error to destroy them and notify the CDPH ISO immediately. Fax numbers must be verified before sending.

Classified CDPH information must only be mailed using secure methods. Large volume mailings of classified CDPH information must be by a secure, bonded courier with signature required upon receipt. Disks and other transportable media sent through the mail must be encrypted with a CDPH ISO approved solution.

C. Solution Architecture

1. System Security Compliance

The system must comply with all applicable CDPH security policies and requirements, as well as those specified in the State Administrative Manual (SAM), Public Health Administrative Manual (PHAM) Privacy Act, and any other applicable State or Federal regulation. All security safeguards and precautions must be subject to the approval of the CDPH ISO.

The system may share data with other entities only after all applicable agreements are in place. For example, using a CDPH data release form, Business Associate Agreement, or Data Use Agreement. These agreements must ensure data is protected according to all applicable standards and policies.

Any data which is exported outside the scope of the system and its security provisions (such as exports for statistical analysis) require approval by the CDPH ISO to ensure sufficient security is in place to protect the exported data.

2. Warning Banner

All systems containing CDPH information must display a login warning banner stating that information is classified, activity is logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree and comply with these requirements.

The following warning banner must be used for all access points (such as desktops, laptops, web applications, mainframe applications, servers and network devices):

WARNING: This is a State of California computer system that is for official use by authorized users and is subject to being monitored and/or restricted at any time. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.

LOG OFF IMMEDIATELY, if you do not agree to the conditions stated in this warning.

3. Layered Application Design

Applications must be able to be segmented into a layered application design separating, at a minimum, the Presentation, Application/Business Logic, and Data Access Logic, and Data Persistence/Database layers.

The Presentation, Application/Business Logic, and Data Access Logic layers must be separated physically by a firewall regardless of physical implementation.

Any system request made to the Business logic layer must be authenticated.

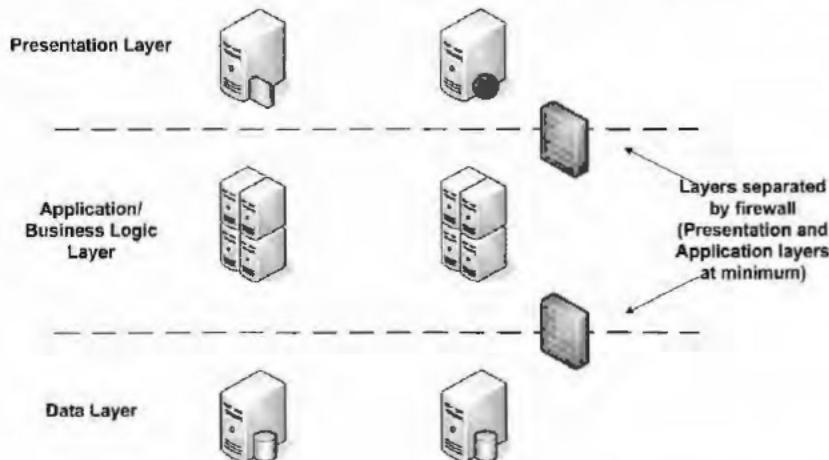
The Data Access Logic Layer may take the form of stored procedures, database Application Programming Interface (API), Data Access Objects/Components, Data Access Middleware, Shared Data Services, or Secure Web Service. Any system request made to the Data Access

logic layer must be authenticated and authorized. No direct access to the Data Persistence/Database layer will be permitted, except through the Data Access logic layer.

All calls to the Data Persistence/Database layer will be made through the Data Access logic layer as a trusted sub-system that utilizes a single database access account to all transactions.

The Data Access Logic Layer must take the form of stored procedures, database API, Data Access Objects/Components, Data Access Middleware, Shared Data Services, or Secure Web Service. System requests made to the Business logic and Data Access logic layers must be authenticated and authorized.

Vendor-provided commercial off-the-shelf (COTS) packages, or components where physical separation of layers is not possible, requires CDPH ISO approval.



4. Input Validation

All user input must be validated before being committed to the database or other application information repository. The system must manage client input controls from server side to the extent possible. Data queries from the Presentation or the Business Logic layers must be validated for appropriate use of query language, and validated for appropriate quantity and quality of data input. This includes In-line Structured Query Language (SQL) calls. The system must validate client input on the server side to the extent possible. All third-party client side input controls must be documented and approved by the CDPH ISO.

5. Data Queries

All Data queries (including In-line SQL calls) will not be allowed from the Presentation or the Business Logic layers unless validated for appropriate use of query language and validated for appropriate quantity/quality of data input. All data queries solution must be approved by the CDPH ISO.

Database table names and column names must not be exposed. Applications must use an alias for every table and column.

Dynamic SQL will not be permitted from the Presentation Layer without prior approval from the CDPH ISO.

6. Username/Password Based Authentication

When usernames and passwords are going to be used as the method for system authentication, the following requirements must be met:

- Username requirements:
 - Must be unique and traceable to an individual.
 - Must not be shared.
 - Must not be hard-coded into system logic.
- Password requirements:
 - Must not be shared.
 - Must be 8 characters or more in length.
 - Must not be a word found in the dictionary, regardless of language.
 - Must be encrypted using irreversible industry-accepted strong encryption.
 - Must be changed at least every 60 days.
 - Must not be the same as any of the previous 10 passwords.
 - Must be changed immediately if revealed or compromised.
 - Must be composed of characters from at least three of the following four groups from the standard keyboard:
 - Upper case letters (A-Z);
 - Lower case letters (a-z);
 - Numbers (0 through 9); and
 - Non-alphanumeric characters (punctuation symbols).
- Account security:
 - Accounts must be locked after three (3) failed logon attempts.
 - Account lock-out reset timers must be set for a minimum of 15 minutes.
 - Accounts must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password.

7. Administrative / Privileged Accounts Management

A privileged account is an account that allows an individual to perform maintenance on an operating system or applications (e.g. create/remove users, install applications, create/modify databases, etc.). Privileged accounts require the approval of the individual's manager, the CDPH ISO, and must include a business justification stating why privileged access is required and what it will be used for. Individuals granted privileged accounts must have already signed the Security and Confidentiality Acknowledgement Statement. (Contact the CDPH ISO for the current version of the Security & Confidentiality Acknowledgement Statement in use.)

The use of shared privileged accounts (e.g. Administrator) is strictly prohibited.

System administration must be performed using a different username rather than the one used for daily non-administrative activities. Administrative accounts must be used only for administrative activity within the authorized role of that account and the individual using it. It must be logged out of immediately after administrative work is complete.

- Username requirements:
 - Must be unique and traceable to an individual.
 - Must not be shared.
 - Must not be hard-coded into system logic.
 - Must be the same across different zones (e.g. Web Zone, Internal network, and Test Labs / Environments).
 - The default built-in Administrator account must be renamed and disabled.

- The naming convention for privileged accounts must not make it obvious that usernames belong to privileged accounts.
- If a generic privileged account is created:
 - Must only be used in an Emergency.
 - Must not be used for routine maintenance.
 - The password storage and management process for generic privileged accounts must be approved by the CDPH ISO.
- Password requirements:
 - Must not be shared.
 - Must be 12 characters or more in length.
 - Must not be a word found in the dictionary, regardless of language.
 - Must be encrypted using irreversible industry-accepted strong encryption.
 - Must be changed at least every 60 days.
 - Must not be the same as any of the previous 10 passwords.
 - Must be changed immediately if revealed, or compromised.
 - Must be comprised of characters from at least three of the following four groups from the standard keyboard:
 - Upper case letters (A-Z);
 - Lower case letters (a-z);
 - Numbers (0 through 9);
 - Non-alphanumeric characters (punctuation symbols).
 - Must be changed immediately upon the termination or transfer of an employee with knowledge of the password.
 - Must not be the same across different zones (e.g. Web Zone, Internal network, and Test Labs / Environments).
- Account security:
 - Accounts must be locked after three (3) failed logon attempts.
 - Account lock-out timers must be set for at least 60 minutes.

8. Service Accounts Management

A service account is an account used to run a service and whose password is known by multiple individuals. When and where it is necessary to use a service account, the account request will be approved by the manager of the Project/Program requesting the account and by the CDPH ISO. Requirements, stating the need for a service account, will be documented in the request. A service account password is shared among the individuals authorized to access the account, and is subject to controls as stated in the password requirements in this document.

Restrictions for Service Accounts

- Sharing passwords via email is prohibited, unless the body of the email itself is encrypted using strong encryption.
- When users are no longer authorized to access an existing service account, the service account password must be changed.

9. Authentication and Authorization

Any system deployed during a project, or as a result of a project, must provide secure role-based access for authorization (separation between system/server administrators and application/database administrators) utilizing the principle of least privilege at all layers/tiers.

In all cases, applications must default to explicitly deny access where authentication and/or authorization mechanisms are required. No application that requires a login can offer to, or be capable of, remembering a user's credentials.

10. Authentication Logging

The system must log success and failures of user authentication at all layers as well as log all user transactions at the database layer as required by regulation, policy or standard, and as prescribed for the given application/system. This logging must be included for all user privilege levels including, but not limited to, systems administrators. This requirement applies to systems that process, store, and/or interface with CDPH information.

11. Automatic System Session Expiration

The system must provide an automatic timeout, requiring re-authentication of the user session after 20 minutes of inactivity.

12. Automatic System Lock-out and Reporting

The system must provide an automatic lock-out of users and a means to audit a minimum of three (3) failed log-in attempts. The means of providing audit information must be approved by the CDPH ISO.

13. Audit (Access)

All systems/applications will implement role-based access to auditing functions and audit trail information utilizing the principle of least privilege.

All systems/applications will implement a secure online interface to Audit Capabilities and Reporting by way of API or network service (or Web Service) to allow CDPH ISO to view logs, auditing procedures, and audit reporting.

14. Audit (Minimum Information)

The minimum log information below is required for any system that contains, or is involved in the transmission of, classified information. The log information should be available on every system running a production environment. This information must be provided upon request of the CDPH ISO for investigations and risk assessments.

The system must record, at minimum, the following events and any other events deemed appropriate by the CDPH ISO:

Transaction Types

- Any and all administrative changes to the system (such as administrative password changes, forgotten password resets, system variables, network configuration changes, disk sub-system modifications, etc.).
- Logon failures.
- Logons during non-business hours.
- Failed access to an application or data.
- Addition, deletion, or modification of users or program access privileges.
- Changes in file access restrictions.
- Database addition, deletion, or modification.
- Copy of files before and after read/write changes.
- Transaction issued.

Individual audit trail records must contain the information needed to associate each query transaction to its initiator and relevant business purpose. Individual audit trail records should capture, at a minimum, the following:

Minimum Audit Trail Record Content

- Date and time stamp.
- Unique username of transaction initiator.
- Transaction recorded.
- Success or failure of transaction recorded.
- Relevant business process or application component involved.
- Data captured (if any).

Audit Trail logs must be maintained at minimum for three (3) years after the occurrence, or a set period of time determined by the CDPH ISO that would not hinder a detailed forensic investigation of the occurrence. The CDPH ISO has final approval authority.

15. Application Security Controls

For any application which accesses classified information, the following technical controls must be present, unless an exception is granted by the CDPH ISO:

- Must use *least privileged accounts* to execute code and to access databases.
- User access rights must be authenticated and authorized on entry to each application tier.
- All user input must be validated, including parameters passed to all public web service methods.
- Information that is not required must not be exposed.
- If a web application fails, it must not leave sensitive data unprotected or expose any details in error messages presented to the user. Any exceptions must be logged or emailed to the appropriate team member.
- Any sensitive data stored in session, cookies, disk files, etc., must be encrypted. Any sensitive data passed between tiers must be encrypted or must use SSL.
- Applications must be protected from the Internet by a front-end web application, firewall, gateway, and proxy of a type approved by the CDPH ISO, which must be included in the documented system design.
- Postback Universal Resource Locators (URLs) must not contain unencrypted record identifiers or database keys.
- Postback URLs must not include query strings.

16. Application Code Security

Application developers should use tools and methods during development to ensure all custom source code is free from security vulnerabilities. At a minimum, the application must be free of the vulnerabilities described in the CWE/SANS Top 25 Most Dangerous Programmer Errors (<http://www.sans.org/top25errors/>).

CDPH has the right to conduct a vulnerability scan against the application prior to its activation, and may disapprove use of the application until the vulnerabilities are remediated and the application re-tested. Any verified vulnerabilities from this list must be corrected by the organization which developed the application, at no additional cost to CDPH. Unless an exception is granted by the CDPH ISO, vulnerabilities identified within third-party components must be remediated by the third-party vendor at no additional cost to CDPH. Otherwise, a different third-party component must be selected and implemented.

17. Strong Authentication

Any information system providing access to Personally Identifiable Information (PII) and/or classified information from the Internet must assess the need for additional strong authentication, to prevent a significant data breach if a password is compromised. Strong authentication is defined as additional mandatory authentication over and beyond the password, for each account which has direct access to PII and/or classified information, or which has administrative privileges. The following factors should be included in the assessment:

- Applicable policies and regulations.
- Sensitivity of the PII or classified information.
- Number of data records.
- Number of user accounts with access to data.
- Level of control over end users.
- Level and frequency of log monitoring.
- Automated alerts and controls for unusual data access patterns.
- End user training on security practices.
- Other mitigating security controls.

The Project/Program providing access to PII and/or classified information from the Internet must either implement an approved strong authentication method, or document why strong authentication will not be utilized. This documentation must be provided to the CDPH ISO for review and approval.

The following methods are approved for strong authentication:

- **Physical Token:** A physical device in the possession of the account holder, which must be physically connected to the computer. Examples include a USB token or Smartcard.
- **One Time Password (OTP):** A temporary one time pass code is provided to the account holder, either by a physical device in their possession, or by way of a pre-defined communication channel such as cell phone or e-mail address. Examples include OTP token, or OTP sent via SMS text message, e-mail, or by automated voice call.
- **X.509 Certificate:** A digital certificate which has been installed on the access point computer or device, utilizing a Public Key Infrastructure (PKI).
- **Firewall Rules:** Firewall TCP/IP rules which ensure the account is only usable from an authorized access point, based upon specific IP address or IP subnet.

The following strong authentication method is approved for personal data access, where accounts have access to only the account holder's personal data, or a single data record they are custodian over such as a family member or information about their company. For example, an application where a client can submit or edit an enrollment form for themselves or someone else, but cannot access any other data records.

- **Personal Challenge Questions:** During registration, the account holder pre-answers one or more questions known only to them. When logging into a different computer, typically tracked with a cookie, they cannot login without correctly answering the pre-configured questions. The user should be prompted for whether the new computer is trusted vs. a one-time login, and this information used to determine whether to save a new cookie.

The proposed strong authentication mechanism must be included in the detailed design documentation as described in Section E.5, Application Security Approvals.

D. Documentation of Solution

1. System Configuration

Project/Program must document and maintain documentation for the system/application. This should include the following:

- Detailed design.
- Description of hardware, software, and network components.
- Special system configurations.
- External interfaces.
- All layers of security controls.

2. Information Classification

Project/Program will document and maintain an information classification matrix of all information elements accessed and/or processed by solution.

The matrix should identify at a minimum:

- Information element.
- Information classification/sensitivity.
- Relevant function/process, or where is it used.
- System and database, or where is it stored.

3. System Roles and Relationships

Project must document the following roles and ensure everyone understands their role, and complies with all applicable policies and regulations.

- The designated owner of the system.
- The designated custodian(s) of the system.
- The users of the system.
- The security administrator for the system.
- Outside entities sending or receiving data to system.

Project must document the organizational structure and relationships between these roles.

4. Audit Method Documentation

Project/Program will document the solution's auditing features and provide samples of audit reporting.

5. Retention of Documentation

The system/application administrators will retain documentation, including audit and activity logs, for a minimum of three (3) years (up to seven (7) years maximum) from the date of its creation or the date it was last in effect, whichever is later. Shorter retention periods must be allowed contingent upon applicable regulations, policies, and standards, and upon approval by the CDPH ISO. In certain circumstances the retention period must be lengthened to comply with regulatory requirements.

E. ISO Notifications and Approvals

1. Security Compliance Notification

As part of each project, assigned staff will document how the proposed solution meets or addresses the requirements specified in this document. This documentation must be submitted to the CDPH ISO prior to taking custody of CDPH information.

2. Notification of Changes to Solution

Once a project is approved as final by the CDPH ISO, no changes will be made to the project scope, documentation, systems or components without a change approval by the CDPH ISO.

3. Notification of Breach

The system/application administrators must immediately, and in writing, report to the CDPH ISO any and all breaches or compromises of system and/or information security. They must also take such remedial steps as may be necessary to restore security and repair damage, if any.

In the event of a breach or compromise of system and/or information security, the CDPH ISO may require a system/application security audit. The CDPH ISO must review the recommendations from the security audit, and make final decisions on the steps necessary to restore security and repair damage.

The system/application administrators must properly implement any and all recommendations of the security audit, as approved by the CDPH ISO.

4. Project Security Approvals

Projects must ensure checkpoints throughout the System Development Life Cycle (SDLC) which verify security requirements are being met. This must be incorporated in the project plan along with identification of necessary resources, timelines, and costs to address these requirements. The CDPH ISO should be involved throughout the SDLC to ensure this occurs.

For reportable Feasibility Study Reports (FSRs), the California Office of Information Security (OIS) requires submission of the *Questionnaire for Information Security and Privacy Components in Feasibility Study Reports and Project-Related Documents*.

See

http://www.cio.ca.gov/OIS/Government/documents/docs/Info_Sec_and_Priv_Components_FSR-Questionnaire.doc.

The response to this document must be approved by the CDPH ISO prior to submission.

Projects must ensure all applicable security requirements and deliverables are included in the project plan, and that ISO approvals are obtained, where required. This includes those listed in the following section, and any covered by other sections of this document. The CDPH ISO must be given reasonable time to review and comment on these deliverables.

5. Application Security Approvals

At a minimum, for any application which accesses classified information, the following documented CDPH ISO approvals must be obtained at the appropriate project phases, and before the application is moved to production.

- CDPH ISO approval of a dated, detailed design document. This design must include network layout including specific firewall port requirements, server hosting locations, operating systems, databases, data exchange interfaces, and points of authentication/authorization. The project must not move beyond the design phase until there is a CDPH ISO approved design.
- CDPH ISO approval of any non-standard development tools (such as programming languages or toolkits).
- CDPH ISO approval of a plan for an independent security code review which addresses at minimum the current Open Web Application Security Project (OWASP) top ten application vulnerabilities, and CWE/SANS Top 25 Most Dangerous Programmer Errors, where applicable. CDPH ISO must approve any findings of that code review not being corrected. CDPH ISO recommends the security code review be carried out during the development process rather than only at the end.
- CDPH ISO approval of a plan for security code reviews of future maintenance code changes, which addresses at minimum the current OWASP top ten application vulnerabilities, CWE/SANS Top 25 Most Dangerous Programmer Errors, where applicable.
- CDPH ISO approval of a plan for an independent automated security vulnerability assessment of the application, and approval of the findings of that assessment. The assessment must assess at minimum the OWASP top ten risks and CWE/SANS Top 25 Most Dangerous Programmer Errors, where applicable.

Independent as indicated above is defined as organizationally separate from those developing or configuration the application. The independence and skill level of the entities being utilized must be approved by the CDPH ISO.

Application code and infrastructure is subject to a CDPH ISO audit, and must match the approved detailed design.

F. Appendix A – SR1 Exemption Form

REF	Security Requirement	Exemption (Yes, No, or N/A)	Business Justification
A	Administrative / Management Safeguards		
1	Workforce Confidentiality Statement		
2	Access Authorization & Maintenance		
3	Information System Activity Review		
4	Periodic System Security & Log Review		
5	Disaster Recovery Plan		
6	Change Control		
7	Supervision of Information		
8	Escorting Visitors		
B	Technical and Operational Safeguards		
1	System Security Compliance		
2	Malware Protection		
3	Patch Management		
4	Encrypted Electronic Transmissions		
5	Encrypted Data Storage		
6	Workstation / Laptop Encryption		
7	Removable Media Encryption		
8	Secure Connectivity		
9	Intrusion Detection and Prevention		
10	Minimum Information Download		
11	Information Sanitization		
12	Removal of Information		
13	Faxing or Mailing of Information		
C	Solution Architecture		
1	System Security Compliance		
2	Warning Banner		
3	Layered Application Design		
4	Input Validation		
5	Data Queries		
6	Username/Password Based Authentication		
7	Administrative / Privileged Accounts Management		
8	Service Accounts Management		
9	Authentication and Authorization		
10	Authentication Logging		
11	Automatic System Session Expiration		
12	Automatic System Lock-out and Reporting		

REF	Security Requirement	Exemption (Yes, No, or N/A)	Business Justification
13	Audit (Access)		
14	Audit (Minimum Information)		
15	Application Security Controls		
16	Application Code Security		
17	Strong Authentication		
D	Documentation of Solution		
1	System Configuration		
2	Information Classification		
3	System Roles and Relationships		
4	Audit Method Documentation		
5	Retention of Documentation		
E	ISO Notifications		
1	Security Compliance Notification		
2	Notification of Changes to Solution		
3	Notification of Breach		
4	Project Security Approvals		
5	Application Security Approvals		