STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT
STD 213 (Rev. 03/2019)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
19-11083	

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

Analytica Consulting, LLC

2. The term of this Agreement is:

START DATE

April 13, 2020 or upon final approval by CDPH, whichever is later

THROUGH END DATE

April 12, 2021

3. The maximum amount of this Agreement is:

500,000.00 (Five 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	8
	Attachment 2	Agency Special Provisions	3
	Attachment 2A	Cost Worksheeet	1
+ -	Attachment 2B	Invoice Format (Sample)	1
+ -	Attachment 2C	Work Order Authorization (Sample)	2
+ -	Attachment 3	Information Technology General Provisions (GSPD-401IT)	12
+ -	Attachment 4	Contractor's Release	1
+ -	Attachment 5	Resumes	10
+ -	Attachment 6	IPSR	10
+ -	Attachment 7	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

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.)

Analytica Consulting, LLC

CONTRACTOR BUSINESS ADDRESS	CITY	STATE	ZIP
9810 Scripps Lake Drive, Suite F	Sacramento	CA	92131
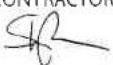
PRINTED NAME OF PERSON SIGNING	TITLE
Steve Rimar	CEO

CONTRACTOR AUTHORIZED SIGNATURE	DATE SIGNED
	04/13/2020

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 03/2019)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
19-11083	

STATE OF CALIFORNIA

CONTRACTING AGENCY NAME

California Department of Public Health

CONTRACTING AGENCY ADDRESS	CITY	STATE	ZIP
1616 Capitol Avenue, Suite 74.262, MS 1802, PO Box 997377	Sacramento	CA	95899

PRINTED NAME OF PERSON SIGNING	TITLE
Kristy Lieu	Chief, Contract Management Unit

CONTRACTING AGENCY AUTHORIZED SIGNATURE	DATE SIGNED
Kristy Lieu	4/13/20

CALIFORNIA DEPARTMENT OF GENERAL SERVICES APPROVAL	EXEMPTION (If Applicable)
	PCC 1102 Emergency Services Executive Order N-25-20

ATTACHMENT 1
STATEMENT OF WORK

A. STATEMENT AND DESCRIPTION

This Statement of Work (SOW) reflects the services the Contractor shall provide to California Department of Public Health (CDPH). Contractor agrees to provide to the CDPH the services described herein.

The Contractor is to design, develop and update dashboards that can be used by the public, and by stakeholders across multiple agencies. In addition, the contractor will provide development of new dashboards and enhancement of existing dashboards in response to the Governor's executive order to fight COVID-19. The dashboards will provide necessary information on the COVID-19 outbreak, spread and response. As stated on the proclamation, "the emergency proclamation includes provisions that protect consumers against price gouging, allow for health care workers to come from out of state to assist at health care facilities, and give health care facilities the flexibility to plan and adapt to accommodate incoming patients." This function is necessary to save valuable time for stakeholders across multiple agencies, determining responder's immediate action and decision making to prevent or mitigate the loss or impairment of life, property, or essential public services, pursuant to PCC 1102.

B. SERVICE LOCATION

The services shall be performed at 1615 Capitol Avenue, Suite 73.373, Sacramento, CA 95814 or at the Contractor's office location at 8910 University Center Lane, Suite 400, San Diego, CA 92122.

C. SERVICE HOURS

The services shall be provided during the normal 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 the Contractor and the State agree that services are required outside regular working hours for specific activities (e.g., batch monitoring, build deployment, software upgrades).

D. PROJECT REPRESENTATIVES

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

California Department of Public Health	Analytica Consulting, LLC
John Buffington, DPM II Telephone: (916) 650-6444 Fax: (916) 650-6420 E-mail: John.Buffington@cdph.ca.gov	Steve Rimar, CEO Telephone: (858) 472-9311 Fax: (858) 272-8260 E-mail: steverimar@analyticaconsulting.com

2. Direct all inquiries to:

California Department of Public Health	Analytica Consulting, LLC
Emergency Preparedness Office Attention: Phebe Lapinig 1615 Capitol Ave. MS 7002 Sacramento, CA 95814 Telephone: (916) 650-6450 Fax: (916) 650-6420 E-mail: Phebe.Lapinig@cdph.ca.gov	Attention: Steve Rimar, CEO 8910 University Center Lane, Suite 1100 San Diego, CA 92122 Telephone: (858) 472-9311 Fax: (858) 272-8260 E-mail: steverimar@analyticaconsulting.com

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

Remittance Address
Contractor: Analytica Consulting, LLC Attention: Steve Rimar, CEO Address: 9810 SCRIPPS LAKE DRIVE, SUITE F San Diego Zip: 92131 Telephone: (858) 472-9311Fax: (858) 272-8260 E-mail: steverimar@analyticaconsulting.com

4. 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 Payee Data Record (STD 204) form, which must match the invoice address in order to avoid payment delays.

E. PROGRESS REPORTS OR MEETINGS

1. Contractor shall submit progress reports or attend meetings with state personnel at intervals determined by CDPH to determine if the Contractor is on the right track, whether the project is on schedule, provide communication of interim findings, and afford occasions for airing difficulties or special problems encountered so that remedies can be developed quickly.

2. At the conclusion of this agreement and if applicable, Contractor shall hold a final meeting at which Contractor shall present any findings, conclusions, and recommendations. If required by this agreement, Contractor shall submit a comprehensive final report.

F. SERVICE TO BE PERFORMED

The Contractor is expected to provide the following services under this contract:

1. Design, develop and enhance Tableau dashboards that satisfy the following requirements:

   a. Web-based dashboards accessible via browser on any desktop or mobile device including tabular details of the COVID-19 impacted facilities. These facilities have high

concentrations of vulnerable Californians and as a result, have a higher probability than other facilities of needing emergency support services from the state.

b. Utilization of source data from other systems/agencies including visualization depicts the total number of facilities with COVID-19 patients, the facilities by department with COVID-19 patients (CDPH and DSS), the facility types with COVID-19 patients (Adult Day Health Care, Intermediate care Facility/Developmentally Disabled - Nursing, Skilled Nursing Facility, Adult Residential, and Residential Care for the Elderly), and facilities by county with COVID-19 patients.

c. Ongoing refreshes of source data, as requested.

d. Leveraging of geographical data and geocoding to highlight and pinpoint affected geographic areas on interactive maps, as requested.

2. Develop, test, implement and maintain public facing and internal Tableau sites in support of the CDPH program areas.

3. Perform data management for Tableau sites in support of the CDPH program areas including developing and maintaining data models, data dictionaries, database structure, views, stored procedures, data transformation, data mapping, data imports, and data refresh, as requested.

4. Develop metrics for monitoring the success of different program areas including the Enterprise Roadmap implementation and improvements, as requested.

5. Perform knowledge transfer including administration, development and configuration.

6. Develop NC4 data transformation, processing and integration for the CDPH program area utilizing CDPH ITSD supported infrastructure and technologies.

7. Extend NC4 data transformation, processing and integration for the DSS and DHCS program areas utilizing CDPH ITSD supported infrastructure and technologies.

8. Cohesive dashboard that combines all data.

9. Summarized executive level report that tracks status changes.

10. Develop and refine processes to allow CDPH to create and sustain dashboards for future events.

11. Gather and document requirements for Tableau sites in support of the CDPH areas, including defining impacts of disasters to facilities.

12. Support data transformation, processing and integration required for CDPH program area reporting, using SAS and SQL Software.

13. Perform data management for Tableau sites in support of the CDPH program areas including developing and maintaining data models, data dictionaries, data base structure, views, stored procedures, data transformation, data mapping, data imports, and data refresh.

14. Develop, test, implement and maintain public facing and internal Tableau sites in support of the CDPH program areas.

a. Develop metrics for monitoring the success of different program areas including the Enterprise Roadmap implementation and improvements.

b. Provide CDPH with Tableau sites, which are embedded in customer-facing websites to better document and information customers of CDPH facilities status during emergency events.

c. Perform knowledge transfer including administration, development and configuration.

G. 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.

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 prior to beginning work. Once the work is complete, the CDPH Contract 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.

1. WOA Procedures

A sample WOA form is included as Attachment 2C.

Table 1 below provides the procedures for creating and processing a WOA.

Table 1

Step	Description	Who
1	The CDPH Contract Manager will work with the Contractor prior to sprint planning session to identify the work to be done and provide a "not to exceed" estimate of hours on the Work Order Authorization Form.	CDPH Contract Manager and Contractor
2	The CDPH Contract Manager will manage the process of gaining approvals on the form authorizing work to begin.	CDPH Contract Manager, Program Designee and Contractor
3	The CDPH Contract Manager will review the WOA during the sprint review session. The team will accept completed work products and determine the disposition of rejected work products. Signatures will be obtained for completion of work that authorizes invoices to be submitted and payment to be made.	CDPH Contract Manager, Program Designee and Contractor
4	CDPH Contract Manager will forward finalized WOAs to Contractor requesting submission of invoices.	CDPH Contract Manager, Program Designee and Contractor
5	The Contractor will submit the invoice to CDPH attaching the signed WOA and associated time sheets.	Contractor

The Contractor is only entitled to reimbursement for time and materials directly related to properly issued WOAs. 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.

2. WOA APPROVAL

All WOAs shall be subject to the State's acceptance, along with all supporting working 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 a WOA is acceptable. No Work shall be accepted by the State for review without a WOA.

Each WOA shall detail and/or be accompanied at a minimum by:

- A summary description detailing the purpose, objective, or goals to be undertaken by the Contractor.
- A resource-loaded schedule that details the SOW categories and tasks, description, personnel resources, approximate start date and end date, and estimated duration for each task and/or task group. The schedule must contain enough details for CDPH to assess the overall level of effort required to complete the WOA;
- A high level test strategy plan.
- Name of the Contractor personnel to be assigned; the Contractor's estimated hours required to accomplish the purpose, objective or goals; the Contractor's billing rates per work hour; and, the Contractor's total cost for the WOA.
- Identification of all significant material including work product WOAs to be developed by the Contractor and delivered to the State.
- Identification of all significant materials to be delivered by the State to the Contractor;
- Identification of any dependencies; tasks required to be performed by CDPH staff in order to accomplish the tasks described in the WOA
- Identification of infrastructure changes/updates needed, if any.
- Code walkthrough/turnover plan to CDPH staff.
- Acceptance criteria for the work to be performed.

The Contractor will offer its price for a WOA using the rates shown in its RFO response Cost Worksheet, as approved by the State. Personnel resources expended on task accomplishment more than the cost authorized in the WOA will be at no cost to the State. Contractor will be paid only for WOAs deemed complete and as accepted by the State as described in each WOA. Vendor requests for revisions to the estimates included in a WOA must be submitted to CDPH for approval prior to any overages occurring. CDPH will review and approve revisions to the WOA, as appropriate. Any work performed prior to an authorized WOA will not be paid by the State.

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

H. CONTRACTOR ADMINISTRATIVE REQUIREMENTS

1. Contractors Contract Manager

The Contractor shall designate a Contract Manager to whom all project communications may be addressed, who 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 successful completion of the required tasks.

Contractor personnel should continue to keep their knowledge and skills up-to-date throughout the term of the Contract.

2. Contractors 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 ten (10) business 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 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 MSA RFO and SOW, provide a resume and sample work, and must be approved in writing by CDPH.

3. Submission of Invoices

Payment for services performed under this Contract 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 work is concluded and CDPH notifies the Contractor that the WOA work is accepted. One invoice shall be submitted to the CDPH Contract Manager, detailing the labor rate as agreed upon in the Cost Worksheet. No more than one invoice can be processed in a 30-day period. Multiple WOAs can be included on one invoice. A sample Invoice Format is included herein as Attachment 2B.

Invoices submissions must include the following:

a) Company letterhead
b) Submission Date
c) Name, Address and Phone number of the CDPH Contract Manager receiving invoice
d) Invoice Number
e) Contract Number
f) SB/DVBE number, if applicable
g) All WOAs with associated hours, descriptions and total amounts requested
h) Comments, as needed
i) Remittance Information
j) Name, Title, Address and Phone Number, and Signature of Authorized Representative
k) Contractor timesheets, including daily time entries

4. 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:

a) First level: CDPH Contract Manager
b) Second level: CDPH Project Manager
c) Third level: CDPH Information Officer

5. Artifact Format

Unless explicitly stated otherwise, all Artifacts shall be provided 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 will organized, free of spelling or typographical errors, grammatically correct and contain pertinent, up to date information when submitted to CDPH.

6. Return of State Property

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

I. **STATE RESPONSIBILITIES**

CDPH shall:

1. Assign a Contract Manager (CM) to coordinate WOA completion, approval of WOA, and coordinate payment of invoices.

2. Provide the required hardware and software to support a minimum of four (4) environments; Development, Testing, Staging, and Production.

3. Identify a Product Owner (PO) within Program who will be available throughout the duration of the project to provide timely decisions and clarifications on required user stories.

4. Work with the Contractor and provide clarifications of the WOA process and associated expectations.

5. Be responsible for all security assessments.

6. Provide access to appropriate levels of staff, stakeholders, users, and CDPH management for successful completion of project activities.

7. Approve any staffing changes in advance of the change.

8. Promote timely decisions and reviews of WOAs and Work Products.

9. Pay invoices based on CDPH acceptance of approved WOAs.

10. Review invoices and associated documents within ten (10) business days of receipt and notify the Contractor in writing of acceptance or dispute.

11. Provide building access and work space for Contractor staff.

J. SUBCONTACTOR

Subcontractors may not be utilized for this project.

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 approval of the invoices, the State agrees to compensate the Contractor for Time and Materials with the Classification line items amount specified in Attachment 2A – Cost Worksheet.

   C. Invoices shall include the Agreement Number and shall be submitted in triplicate not more frequently than monthly in arrears to:

   Contract 19-11083
   California Department of Public Health
   Emergency Preparedness Office
   Attn: Phebe Lapinig
   1615 Capitol Avenue, MS 7002
   Sacramento, CA 95814

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

   D. Invoice shall be accompanied by a Work Order Authorization (WOA), as identified in Attachment 1 – Statement of Work and contain the following:

   1) Be prepared on Contractor letterhead.
   2) Invoices must be submitted to CDPH either electronically or in hard copies.
   3) Identify the billing and/or performance period covered by the invoice.
   4) Itemize costs 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 CDPH.

   E. Amounts Payable

   The amounts payable under this agreement shall not exceed $500,000 for the term of this agreement.

   F. Rates Payable

   Contractor will be reimbursed for services satisfactorily performed based on the following 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 (30) 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 be clearly marked "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 Pooled Money Investment Fund commencing on the date that an audit or examination finding is mailed to the Contractor, beginning 30 days after Contractor's receipt of the State's demand for repayment.

D. If the Contractor has filed a valid appeal regarding the report of audit findings, 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

No travel shall be permitted under this agreement.

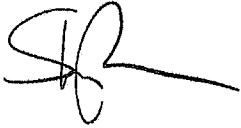## ATTACHMENT 2A
COST WORKSHEET

- List the Name, Project Role, Classification, and hourly rate of the proposed staff, including subcontractors, who will provide the services.
- Attach resume for each proposed staff listed.

Name & Project Role Title	Classification	Subcontractor (yes/no)	Hourly Rate
Adita Zeqollari	IT Consultant	No	$110
Jake Coniglione	IT Senior Consultant	No	$120
Jun Lee	IT Senior Consultant	No	$120
Jennifer De La Cruz	IT Principal	No	$150

1. CDPH has allocated $500,000 for this contract.

2. This is a time and materials (T&M) based Contract. 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 Contractor further understands that the hourly rates must be fully loaded. This includes and is not limited to: operating expenses, labor, transportation/travel costs, equipment costs, supplies, overhead, annual inflation costs/rate adjustments, profit margin, taxes, shipping, and all other fees and costs.

4. No travel will be reimbursed under this contract.

5. Subcontractor may be utilized for this project.

The Contactor hereby certifies that the materials submitted and the hourly rate(s) on this Cost Worksheet are true and accurate to the best of its knowledge and shall remain in effect throughout the term. CDPH reserves the right to amendment for additional time and/or money.

NOTE: Failure to sign this will be deemed non-responsive.

Print Name:	Title of Authorized Representative:
Steve Rimar	CEO and Founder
Signature:	Date:
	04/10/20

ATTACHMENT 2B
INVOICE FORM AT (SAMPLE)
(Must Include Contractor's Company/Business Letterhead)

Invoice Date:

California Department of Public Health
Attn: CDPH Contract Manager Name
Mailing Address:
Sacramento, CA 95899
Phone Number:

Invoice No.:
Contract No.:
SB/DVBE Certification No. (if applicable):

This invoice requests payment of the following Work Order Authorization(s) (WOA):

WOA #	Hours	WOA Description	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									
Agreement #:						WOA #:			
Fiscal Year:				Start Date:				End Date:	
Account	Alt Account	Program	Project ID	Activity ID	Reporting Structure	Service Location	Fund Sub-fund	Actual Cost①	
								$	
						TOTAL ACTUAL COST:		$	

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

*Total actual cost must match invoice. Total cost on the invoice cannot exceed total estimated cost on WOA and must align with 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 Complete 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-Labor Hours Based on Work Description]

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

*Labor rates: must not exceed the approved hourly rates on Attachment 2A, Cost Worksheet.

[CM Obtain Signatures To Authorize Work To Begin]

Organization / Role	Name	Signature	Date
Contractor Manager			
CA Department of Public Health ITSD Project Manager (PM)			
CA Department of Public Health Program Designee			

SECTION 2: Work Order Approval to Invoice

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

- Invoiced hourly rate aligns with agreement.
- Invoiced costs do not exceed **Total Estimated Costs** for this WOA.
- Staff timesheets provided match 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 ITSD Contract Manager			

Note: Invoices must include Contractor timesheets and cannot exceed "Total Estimated Cost" listed on page 1 of this WOA.

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.

   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.

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:

    a) 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);

    b) Contract form, i.e., Purchase Order STD 65, Standard Agreement STD 213, etc., and any amendments thereto;

    c) Other Special Provisions;

    d) Statement of Work, including any specifications incorporated by reference herein;

    e) Cost worksheets; and

    f) All other attachments incorporated in the Contract by reference.

12. **PACKING AND SHIPMENT:**

    a) 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:

       i) show the number of the container and the total number of containers in the shipment; and

       ii) the number of the container in which the packing sheet has been enclosed.

    b) 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.

    c) 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.

    a) 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.

    b) 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.

    c) 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:

    a) 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.

(REVISED AND EFFECTIVE 9/5/14)

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 it's 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 certificates(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 sub-section 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.

(REVISED AND EFFECTIVE 9/5/14)

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

(REVISED AND EFFECTIVE 9/5/14)

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 REQUIRMENTS:** 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).).

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** _19-11083_ 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): Analytica Consulting, LLC _____

Signature of Contractor or Official Designee: _____ Date: _____

Printed Name/Title of Person Signing: _____

CDPH Distribution: Accounting (Original) Program

CDPH 2352 (7/07) Page 1 of 1

ADITA ZEQOLLARI

aditazeqollari@analyticaconsulting.com • ███████

Summary of Qualifications

Adita holds an M.S. in Data Science & Engineering from the University of California, San Diego and a B.S. in Financial Mathematics and Statistics from the University of California, Santa Barbara. Adita has 10 years of experience in multiple sectors including healthcare, biotech, and education. Her expertise spans a variety of data analytics areas including machine learning, natural language processing, data visualization, and data management, as well as, data analytics tools including Python, Apache Spark, SAS, Tableau, Alteryx, SQL, Oracle BI, and IBM Cognos.

Professional Work Experience

Analytica Consulting – San Diego, CA   2019 - Present
Data Engineering & Analytics Consultant

- North County Health Services (NCHS) - Developed a large-scale centralized data & analytics solution for physicians to receive automated reports containing vital information on high risk patients. Developed the data layer, which automated the ETL and statistical processes by utilizing Python. Collaborated with the NCHS internal team to deliver the solution to healthcare providers across the NCHS system.
- Edwards Lifesciences – Developed a sales operations analytics solution which integrated data from Salesforce, eSales (custom data warehouse) and a proprietary financial system. The solution provided role-based security enabling both internal and external Edward's sales reps to see their sales performance by client, territory and product.
- California Community College League (CC League) – Developed a performance funding statistical and simulation model which enabled the client to allocate funds appropriately.

Stanford University, School of Medicine, Strategy and Analytics – Stanford, CA   2017 – 2019
Strategic Insights Analyst

- Designed and delivered analyses utilizing internal data combined with external data, obtained through web-scraping and APIs, to inform strategic initiatives in the Stanford Medicine network (Stanford Medical School and Stanford hospitals)
- Reversed engineered the U.S. News and World Report medical school rankings utilized in strategic initiatives to improve Stanford's position
- Consulted with departments and divisions in Stanford Medicine to identify and implement analytical solutions

Stanford University, Institutional Research & Decision Support – Stanford, CA   2015 – 2017
Institutional Research Analyst

- Consulted with internal and external stakeholders to design analyses and visualizations, define information needs, and deliver analyses related to Stanford students and faculty (demographics, enrollment, degrees, compensation) using R, Tableau, SQL, and Oracle BI
- Worked closely with Stanford's IT organization to assist with the development of a new student reporting system by designing dashboard specifications, gathering user requirements, providing subject matter expertise, testing, and resolving data issues
- Lead comparative faculty salary analyses examining faculty salaries by department and rank, compiling data from peer institutions to ensure Stanford's competitiveness in hiring / retaining faculty and to support diversity initiatives

Massachusetts Institute of Technology, Data Management – Cambridge, MA   2013 – 2016
Business Intelligence Analyst
- Collaborated extensively with the Office of the Provost to identify and deliver university-wide data analytics solutions
- Utilized IBM Cognos and Tableau in an Agile environment to develop dozens of analyses and dashboards for administration, faculty, and other users to support decision-making covering subjects such as finance, HR, research and admissions
- Developed and administered training classes, user groups, and demos to empower users to implement available and emerging software to streamline business processes and gather insights from data

Massachusetts Institute of Technology, School of Engineering – Cambridge, MA   2012 – 2013
Financial Assistant in Research Administration
- Responsible for the fiscal management of 15 engineering faculty members' research accounts
- Worked closely with professors, MIT's Office of Sponsored Programs, and sponsors to prepare and submit grant proposals
- Abbott Vascular, Operations and Site Services – Temecula, CA 2011 – 2012 Financial Analyst
- Analyzed budget variances using SAP and in-house data management and BI systems to provide insight to senior leadership
- Prepared monthly analyses of operational results with comparison to forecast to support operational cost-saving projects
- Generated analyses compiling data across several systems to support audits and ensure compliance with FDA requirements

Education and Certifications
University of California – San Diego, CA
M.S. Data Science & Engineering

University of California Santa Barbara – Santa Barbara, CA
B.S. Financial Mathematics and Statistics

Harvard University Extension School – Cambridge, MA
Courses: Organizational Behavior, Financial Statement Analysis, Investment Theory and Applications, Nonprofit Accounting

JENNIFER DE LA CRUZ
Director of Data Engineering & Analytics
jenniferdelacruz@analyticaconsulting.com • ▮▮▮▮▮▮▮

Summary of Qualifications

As Director of Analytics, Jennifer manages Analytica's consulting organization and is responsible for the delivery of all client projects. She is an accomplished data professional with over 35 years of experience in consulting and industry. Jennifer holds a master's degree in data science and engineering from UC San Diego, an MBA from Wharton, and a master's degree in engineering from Stanford University. She is also certified as a Lean Six Sigma Master Black Belt.

Jennifer has a passion for using statistics and data science to solve complex, high-value business problems. Her experience spans a range of functions including financial management, process improvement, operations management, product development and product quality. Jennifer's industry strengths lie in information systems, financial services, healthcare, engineering, manufacturing, and insurance.

Professional Work Experience

Analytica Consulting – San Diego, CA   2019 – Present
Director of Data Engineering & Analytics
Jennifer manages Analytica's consulting organization and is responsible for the delivery of all client projects, including:

- Rady Children's Hospital San Diego (RCHSD) – Led the design and development of a centralized data analytics solution to help improve hospital operations
- California Department of Public Health – Led the design and development of several data & analytics projects for the Center of Healthcare Quality and Emergency Preparedness Office.
- Illumina – Led the design and development of several data & analytics projects for the Commercial, Global Quality & Operations, and Manufacturing divisions.
- Qualcomm Employee Diversity and Global Climate Survey Studies – Led the design and development of two HR studies for Qualcomm.
- Becton Dickenson (BD) – Led the design and development of an unsupervised machine learning model using natural language processing to improve product failure classification
- California Community College League (CC League) – Led the design and development of a CEO Tenure and Retention study as well as a Student Performance Funding study.

University of California San Diego – San Diego, CA   2016 – 2018
Master's Thesis Project, Data Science and Engineering: Network Analysis of Political Data

- Designed data model of political situations as network graphs and developed graph database to support solution by constructing working data pipeline that parsed 17 thousand newspaper articles using Stanford CoreNLP natural language processing and transformed annotations into political network of senators of 115th U.S. Congress
- Presented results at UC San Diego to members of Computer Science and Engineering Department, Political Science Department, San Diego Supercomputer Center, and local data science community

IBM Corporation
Data Science Engineer 2017
Business Process Owner of Global Travel and Expense Reimbursement, HQ 2010 - 2016
Global Travel Expense Controller, IBM Corporate HQ 2008 - 2010
Senior Managing Consultant, IBM Global Business Services 2002 – 2008

- Used complex data mining and predictive statistical modeling to understand patterns of policy non-compliance within large quantities of expense reimbursement data, and developed risk scoring models to detect anomalies
- At IBM Research laboratory, used SQL queries to extract training and test data from multiple tables in large database and applied machine learning techniques of AI to develop classifier that aggregates business travel expenses, then collaborated with team of data scientists to integrate classifier into new, data-driven business solution: intelligence tool that company both sells to clients and uses internally for negotiating volume-based cost savings with suppliers
- Worked directly with senior leaders at consulting clients State Street Bank, Kaiser Permanente, Sprint Nextel and others to identify problems through complex data analysis and deploy solutions for business process improvement
- As IBM-certified Lean Six Sigma Master Black Belt, trained 950 Black Belts, Green Belts and Champions at Fidelity Investments, USAA, Microsoft, and other client companies to convert data into valuable analytics solutions using advanced quantitative methods and statistical modeling techniques such as correlation analysis, regression analysis (linear, non-linear and logistic), analysis of variance, chi-square testing and design of experiments
- Established thought leadership and honed communication skills appropriate for executive-level audiences by writing whitepapers and presenting case studies at conferences of the Institute of Financial Operations, Institute for Defense and Government Advancement, International Quality and Productivity Center, Society of Actuaries, California Association for Healthcare Quality, and other professional organizations, for business development

PricewaterhouseCoopers – San Diego, CA 2000 - 2002
Principal Consultant, PwC Consulting

- Implemented strategic plan for process management at Wellmark Blue Cross and Blue Shield that made process owners accountable for quality metrics and cost
- Trained employees and coached improvement projects in Wellmark call center that saved over half a million dollars while providing better service to two million customers and health care providers

Black & Decker Corporation – Pacoima, CA 1999 – 2000
Director, Six Sigma, Pfister Division

- Implemented Six Sigma initiative for quality improvement and cost reduction at faucet and fixture manufacturer
- Reported directly to President of Pfister Division with dotted line accountability to Black & Decker Vice President
- Led team of five Black Belts in completing projects worth $6 million in scrap elimination, rework reduction, and process streamlining
- Developed multi-level training strategy for 800 employees to introduce culture of continuous improvement
- Presented quarterly results to Black & Decker's President, Six Sigma Global Support Team, and Wall Street analysts

Rain Bird Sprinkler Manufacturing – Tucson, AZ   1997 – 1998
Plant Manager, Sonora Southwest Molding Division
- Directed $5.8-million start-up manufacturer of injection molded sprinkler and irrigation components
- Produced 35 million parts in first year running 24/7 operation
- Expanded plant from 30 thousand square feet to 50 thousand square feet, increased capacity from 17 to 33 presses between 40 and 500 tons in size, and increased workforce from 100 to 180 employees
- Managed and recruited leadership team including highly-qualified managers of production, quality, materials, and manufacturing engineering

Protogenesis – Carlsbad, CA   1990 – 1997
President
- Founded company to develop new products and manufacture prototypes, molds, tooling, and fixtures using computer-aided design and computer-aided manufacturing (CAD/CAM) and CNC machining
- Served 300 corporate and professional clients
- Grew sales at equivalent rate of 30% per year over five years
- Built company into entity with strong market value, then negotiated its acquisition by multi-million-dollar, privately held customer of company, securing significant returns for principals

Rohm and Haas Company – Philadelphia, PA   Summer 1989
Marketing Associate, Corporate Headquarters
- Developed strategy to introduce engineering thermoplastics additives into blow molding market with demand of over 50 million pounds a year and growing, by targeting key applications for cars, appliances and computers

General Motors Corporation – Warren, MI   1984 - 1988
Senior Process Engineer, General Motors Technical Center
- Developed new manufacturing technology for polymer composite body panels used on first mass-produced mid-engine sports car made by U.S. manufacturer
- Completed one-year management training program with assignments in auto assembly plant, component manufacturing plant, and advanced vehicle design center

Education and Certifications
University of California San Diego – La Jolla, CA
Master of Advanced Study; Major in Data Science and Engineering

The Wharton School, University of Pennsylvania – Philadelphia, PA
Master of Business Administration; Dual Major in Finance and Entrepreneurial Management

Stanford University – Stanford, CA
Master of Science; Major in Chemical Engineering, General Motors Graduate Study Fellowship

University of Michigan – Ann Arbor, MI
Bachelor of Science; Major in Chemical Engineering, Cum Laude

Skills and Abilities

- Python programming language and libraries (scikit-learn, pandas, SciPy) for data science and AI/ML Applications
- Machine learning algorithms (classification, regression, clustering) for finding new solutions to complex problems
- SQL for querying and managing relational data
- Tableau and other techniques for data visualization

JAKE CONIGLIONE
Senior Consultant
jakeconiglione@analyticaconsulting.com • ███████

SUMMARY OF QUALIFICATIONS
Jake is an experienced data analyst and engineer with expertise in developing analytics applications that are accessible to both technical and non-technical business users. He has expertise with several analytics platforms including Tableau and Qlik and has worked with various data sources ranging from relational databases (Oracle, SQL Server, MySQL), commercial applications (Salesforce, Oracle) and custom software. Jake has presented to community leaders, state officials and executives of respected companies.

PROFESSIONAL WORK EXPERIENCE
Analytica Consulting – Sacramento, CA
Senior Consultant   2016 - Present
- California Department of Public Health
  - Lead the design, development, and maintenance of both public-facing and executive-level internal Tableau dashboards to support the analytical and business needs of the Center of Health Care Quality.
  - Works closely with program leadership to understand business requirements, define problems, and provide solutions that consistently meet stakeholder needs.
  - Queried source data systems, recommended and implemented optimized data architecture, and produced analysis-ready data.
- UCSD Health
  - Developed an interactive QlikView application for analyzing stroke risk prevention factors.
- Edwards Life Sciences
  - Developed a QlikView application analyzing Salesforce license usage that provided insights leading to $200k in annual savings.
- Sony
  - Worked closely with Sony's Program Executives on a QlikView application displaying budgetary data for the PlayStation platform.

Nexi – Arcata, CA
Assistant Designer   2014 –2016
- Researched and developed custom electronic solutions for utility metering.
- Provided technical expertise including data analytics, programming, testing, and development.
- Managed intern-team performance and provide weekly memos to the CEO.

EDUCATION AND CERTIFICATIONS
Humboldt State University – Arcata, CA
- B.S. in Environmental Resources Engineering

State of California Certified - Engineer in Training, #159036
Certified Tableau Developer

SKILLS AND ABILITIES
- Expertise using Tableau Desktop, Tableau Server, and QlikView.

- Experience with numerous data source types including Oracle, SQL, and MySQL.
- Able to write VBA macros to automate processes in Word, Excel.
- Experience building dashboards and reports in Salesforce and analyzing Salesforce data.
- Awarded *Meritorious Winner* of the Consortium of Mathematics and its Applications' Annual Interdisciplinary Contest in Modeling in 2016.

Jun Lee

junlee@analyticaconsulting.com • ███████

SUMMARY OF QUALIFICATIONS

Jun is a data analysis expert and BI tools specialist with expertise in Qlik, Tableau, Denodo, JReport, D3, and various other software. He has extensive knowledge in software development, having developed in C, C++, Java, Python, R, SQL, HTML, CSS, JavaScript and various related frameworks/programming environments.

Jun currently works with Fortune 500 companies and software clients by providing BI applications, data solutions and script development.

PROFESSIONAL WORK EXPERIENCE

Analytica Consulting – San Diego, CA
Senior Consultant   2016 – Present

- Illumina
  - Developed semantic layer within Denodo for the Global Quality team analyzing both customer and supplier quality metrics
  - Created Tableau executive dashboards including textual analysis and conditional aggregations.
  - Transitioned data sources of different departments into a modular database capable of building new reports. New key metrics, views, and queries were documented into pdf files.
  - Led onsite Tableau trainings to teams of data architects, IT, support, and business, and created online Tableau support infrastructure.
  - Worked with IT to establish and maintain data governance with Illumina's SAP Hana platform and PostgreSQL database.
- California Department of Public Health
  - Created reporting-level Tableau dashboards with drill-down capability into key metrics. Various flat files of different file types were transformed into a single, flexible Tableau data source.
  - Debugged and improved existing ETL process, including C# files in Visual Studio and .NET framework, to incorporate new application mechanisms. Created additional logging features for section management.
  - Documented and recommended future application changes to security, remote database connection, and functionality to meet new business requirements.
- Franchise Tax Board
  - Developed 12 Section 501 and WCAG 2.0 compliant tax forms in Adobe InDesign.
  - Created form structure, style, and action behavior cross-referencing Adobe and heuristic best practices for accessibility; compiled a checklist adherent to Section 508 for future reference.
  - Tested forms in different environments and assisted-technology for modular and transparent behavior.
- Certona
  - Developed executive dashboards in JReport by creating business views, library components, and customized queries to stored procedures.
  - Formed a new data hierarchy in SQL server and JReport server, including implementation guidelines.
  - Analyzed capabilities of various non-relational databases and provided a data warehouse solution.
- First Place for Youth
  - Developed Python scripts that extract all JSON data objects from a website, and structure the data into a clean format for the client.
  - Set up an automated version of the script via an RDC to an Amazon E2 database, allowing users to freely access a continuously refreshing script.
  - Used multi-threading and abstraction to reduce extraction and transformation process time by over 400%.
- Ingram Micro
  - Worked with business owners and IT professionals to develop functional dashboards with proper data governance in QlikView.
  - Developed a 2-tier layered QlikView data model architecture and automated cluttered flat files and unstructured data sources.
  - Mentored and trained business users and developers on how to support and create QlikView apps.

PROFESSIONAL WORK EXPERIENCE

UCSD BFS Analytics – San Diego, CA

Data Analyst   2012 – 2016

- Developed a web crawler in Python to extract information from sites and transform into a relational database.
- Transformed data (SQL databases, HTML tables, flat files) into flexible data sources capable of front-end analysis.
- Provided predictive modeling and trend analyses in Tableau to UCSD's staff leadership team, on a biweekly basis. Visualized and presented data analyses in Tableau workbooks and dashboards.
- Optimized Tableau queries by merging data sources and recreating nested relationships, reducing load time and improving accuracy of query results. Blended data from query results, creating new insights into the data.

California Cereal Products – Oakland, CA

Web Developer/Designer   2010 – 2012

- Designed and developed California Cereal's website. Outlined and structured layout according to target audience.
- Utilized Google Analytics and Webmaster tools to mark and increase average daily audience from 0 to 35.
- Created sitemaps and tagged keywords in website to improve google search ranking from 13 to 2.
- Presented CCP products, details, and changes to CCP's clients through Adobe Photoshop and Illustrator.

EDUCATION AND CERTIFICATIONS

University of California, San Diego – La Jolla, CA

- B.S. in Computer Science
- B.S. in Cognitive Science

ATTACHMENT 6

Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

This Information Privacy and Security Requirements Exhibit (For Non-HIPAA/HITECH Act Contracts) (hereinafter referred to as "this Exhibit") sets forth the information privacy and security requirements Contractor is obligated to follow with respect to all personal and confidential information (as defined herein) disclosed to Contractor, or collected, created, maintained, stored, transmitted or used by Contractor for or on **behalf** of the California Department of Public Health (hereinafter "CDPH"), pursuant to Contractor's agreement with CDPH. (Such personal and confidential information is referred to herein collectively as "CDPH PCI".) CDPH and Contractor desire to protect the privacy and provide for the security of CDPH PCI pursuant to this Exhibit and in compliance with state and federal laws applicable to the CDPH PCI.

I. <u>Order of Precedence</u>: With respect to information privacy and security requirements for all CDPH PCI, the terms and conditions of this Exhibit shall take precedence over any conflicting terms or conditions set forth in any other part of the agreement between Contractor and CDPH, including Exhibit A (Scope of Work), all other exhibits and any other attachments, and shall prevail over any such conflicting terms or conditions.

II. <u>Effect on lower tier transactions</u>: The terms of this Exhibit shall apply to all contracts, subcontracts, and subawards, and the information privacy and security requirements Contractor is obligated to follow with respect to CDPH PCI disclosed to Contractor, or collected, created, maintained, stored, transmitted or used by Contractor for or on behalf of CDPH, pursuant to Contractor's agreement with CDPH. When applicable the Contractor shall incorporate the relevant provisions of this Exhibit into each subcontract or subaward to its agents, subcontractors, or independent consultants.

III. <u>Definitions</u>: For purposes of the agreement between Contractor and CDPH, including this Exhibit, the following definitions shall apply:

A. <u>Breach</u>:

"Breach" means:

1. the unauthorized acquisition, access, use, or disclosure of CDPH PCI in a manner which compromises the security, confidentiality or integrity of the information; or

2. the same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29(f).

B. <u>Confidential Information</u>: "Confidential information" means information that:

1. does not meet the definition of "public records" set forth in California Government Code section 6252(e), or is exempt from disclosure under any of the provisions of Section 6250, et seq. of the California Government Code or any other applicable state or federal laws; or

2. is contained in documents, files, folders, books or records that are clearly labeled, marked or designated with the word "confidential" by CDPH.

C. <u>Disclosure</u>: "Disclosure" means the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.

D. <u>PCI</u>: "PCI" means "personal information" and "confidential information" (as these terms are defined herein:

E. <u>Personal Information</u>: "Personal information" means information, in any medium (paper, electronic, oral) that:

1.   directly or indirectly collectively identifies or uniquely describes an individual; or

2.   could be used in combination with other information to indirectly identify or uniquely describe an individual, or link an individual to the other information; or

3.   meets the definition of "personal information" set forth in California Civil Code section 1798.3, subdivision (a) or

4.   is one of the data elements set forth in California Civil Code section 1798.29, subdivision (g)(1) or (g)(2); or

5.   meets the definition of "medical information" set forth in either California Civil Code section 1798.29, subdivision (h)(2) or California Civil Code section 56.05, subdivision (j); or

6.   meets the definition of "health insurance information" set forth in California Civil Code section 1798.29, subdivision (h)(3); or

7.   is protected from disclosure under applicable state or federal law.

F.   Security Incident: "Security Incident" means:

1.   an attempted breach; or

2.   the attempted or successful unauthorized access or disclosure, modification or destruction of CDPH PCI, in violation of any state or federal law or in a manner not permitted under the agreement between Contractor and CDPH, including this Exhibit; or

3.   the attempted or successful modification or destruction of, or interference with, Contractor's system operations in an information technology system, that negatively impacts the confidentiality, availability or integrity of CDPH PCI; or

4.   any event that is reasonably believed to have compromised the confidentiality, integrity, or availability of an information asset, system, process, data storage, or transmission. Furthermore, an information security incident may also include an event that constitutes a violation or imminent threat of violation of information security policies or procedures, including acceptable use policies.

G.   Use: "Use" means the sharing, employment, application, utilization, examination, or analysis of information.

IV.   Disclosure Restrictions: The Contractor and its employees, agents, and subcontractors shall protect from unauthorized disclosure any CDPH PCI. The Contractor shall not disclose, except as otherwise specifically permitted by the agreement between Contractor and CDPH (including this Exhibit), any CDPH PCI to anyone other than CDPH personnel or programs without prior written authorization from the CDPH Program Contract Manager, except if disclosure is required by State or Federal law.

V.   Use Restrictions: The Contractor and its employees, agents, and subcontractors shall not use any CDPH PCI for any purpose other than performing the Contractor's obligations under its agreement with CDPH.

VI.   Safeguards: The Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of

CDPH PCI, including electronic or computerized CDPH PCI. At each location wher CDPH PCI exists under Contractor's control, the Contractor 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 Contractor's operations and the nature and scope of its activities in performing its agreement with CDPH, including this Exhibit, and which incorporates the requirements of Section VII, Security, below. Contractor shall provide CDPH with Contractor's current and updated policies within five (5) business days of a request by CDPH for the policies.

VII.   Security: The Contractor shall take any and all steps reasonably necessary to ensure the continuous security of all computerized data systems containing CDPH PCI. These steps shall include, at a minimum, complying with all of the data system security precautions listed in the Contractor Data Security Standards set forth in Attachment 1 to this Exhibit.

VIII.   Security Officer: At each place where CDPH PCI is located,, the Contractor shall designate a Security Officer to oversee its compliance with this Exhibit and to communicate with CDPH on matters concerning this Exhibit.

IX.   Training: The Contractor shall provide training on its obligations under this Exhibit, at its own expense, to all of its employees who assist in the performance of Contractor's obligations under Contractor's agreement with CDPH, including this Exhibit, or otherwise use or disclose CDPH PCI.

A.   The Contractor shall require each employee who receives training to certify, either in hard copy or electronic form, the date on which the training was completed.

B.   The Contractor shall retain each employee's certifications for CDPH inspection for a period of three years following contract termination or completion.

C.   Contractor shall provide CDPH with its employee's certifications within five (5) business days of a request by CDPH for the employee's certifications.

X.   Employee Discipline: Contractor shall impose discipline that it deems appropriate (in its sole discretion) on such employees and other Contractor workforce members under Contractor's direct control who intentionally or negligently violate any provisions of this Exhibit.

XI. Breach and Security Incident Responsibilities:

A. Notification to CDPH of Breach or Security Incident: The Contractor shall notify CDPH **immediately by telephone call plus email or fax** upon the discovery of a breach (as defined in this Exhibit), **and** within **twenty-four (24) hours by email or fax** of the discovery of any security incident (as defined in this Exhibit), unless a law enforcement agency determines that the notification will impede a criminal investigation, in which case the notification required by this section shall be made to CDPH immediately after the law enforcement agency determines that such notification will not compromise the investigation. Notification shall be provided to the CDPH Program Contract Manager, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XI(F), below. If the breach or security incident is discovered after business hours or on a weekend or holiday and involves CDPH PCI in electronic or computerized form, notification to CDPH shall be provided by calling the CDPH Information Security Office at the telephone numberslisted in Section XI(F), below. For purposes of this Section, breaches and security incidents shall be treated as discovered by Contractor as of the first day on which such breach or security incident is known to the Contractor, or, by exercising reasonable diligence would have been known to the Contractor. Contractor shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a employee or agent of the Contractor.

Contractor shall take:

1. prompt corrective action to mitigate any risks or damages involved with the breach or security incident and to protect the operating environment; and

2. any action pertaining to a breach required by applicable federal and state laws, including, specifically, California Civil Code section 1798.29.

B. Investigation of Breach and Security Incidents: The Contractor shall immediately investigate such breach or security incident. As soon as the information is known and subject to the legitimate needs of law enforcement, Contractor shall inform the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer of:

1. what data elements were involved and the extent of the data disclosure or access involved in the breach, including, specifically, the number of individuals whose personal information was breached; and

2. a description of the unauthorized persons known or reasonably believed to have improperly used the CDPH PCI and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the CDPH PCI, or to whom it is known or reasonably believed to have had the CDPH PCI improperly disclosed to them; and

3. a description of where the CDPH PCI is believed to have been improperly used or disclosed; and

4. a description of the probable and proximate causes of the breach or security incident; and

5. whether Civil Code section 1798.29 or any other federal or state laws requiring individual notifications of breaches have been triggered.

C. Written Report: The Contractor shall provide a written report of the investigation to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security

Officer as soon as practicable after the discovery of the breach or security incident. The report shall include, but not be limited to, the information specified above, as well as a complete, detailed corrective action plan, including information on measures that were taken to halt and/or contain the breach or security incident, and measures to be taken to prevent the recurrence or further disclosure of data regarding such breach or security incident.

D.   Notification to Individuals: If notification to individuals whose information was breached is required under state or federal law, and regardless of whether Contractor is considered only a custodian and/or non-owner of the CDPH PCI, Contractor shall, at its sole expense, and at the sole election of CDPH, either:

1.   make notification to the individuals affected by the breach (including substitute notification), pursuant to the content and timeliness provisions of such applicable state or federal breach notice laws. Contractor shall inform the CDPH Privacy Officer of the time, manner and content of any such notifications, prior to the transmission of such notifications to the individuals; or

2.   cooperate with and assist CDPH in its notification (including substitute notification) to the individuals affected by the breach.

E.   Submission of Sample Notification to Attorney General: If notification to more than 500 individuals is required pursuant to California Civil Code section 1798.29, and regardless of whether Contractor is considered only a custodian and/or non-owner of the CDPH PCI, Contractor shall, at its sole expense, and at the sole election of CDPH, either:

1.   electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the Attorney General pursuant to the format. content and timeliness provisions of Section 1798.29, subdivision (e). Contractor shall inform the CDPH Privacy Officer of the time, manner and content of any such submissions, prior to the transmission of such submissions to the Attorney General; or

2.   cooperate with and assist CDPH in its submission of a sample copy of the notification to the Attorney General.

F.   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 verbal or written notice to the Contractor. Said changes shall not require an amendment to this Exhibit or the agreement to which it is incorporated.

CDPH Program Contract Manager	CDPH Privacy Officer	CDPH Chief Information Security Officer
See the Scope of Work exhibit for Program Contract Manager	Privacy Officer Privacy Office Office of Legal Services California Dept. of Public Health 1415 L Street, 5th Floor Sacramento, CA 95814 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	Chief Information Security Officer Information Security Office California Dept. of Public Health P.O. Box 997377 MS6302 Sacramento, CA 95899-7413 Email: cdphiso@cdph.ca.gov Telephone: (855) 500-0016

XII.   Documentation of Disclosures for Requests for Accounting: Contractor shall document and make available to CDPH or (at the direction of CDPH) to an Individual such disclosures of CDPH PCI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of personal information as required by Civil Code section 1798.25, or any applicable state or federal law.

XIII.   Requests for CDPH PCI by Third Parties: The Contractor and its employees, agents, or subcontractors shall promptly transmit to the CDPH Program Contract Manager all requests for disclosure of any CDPH PCI requested by third parties to the agreement between Contractor and CDPH (except from an Individual for an accounting of disclosures of the individual's personal information pursuant to applicable state or federal law), unless prohibited from doing so by applicable state or federal law.

XIV.   Audits, Inspection and EnforcementCDPH may inspect the facilities, systems, books and records of Contractor to monitor compliance with this Exhibit. Contractor shall promptly remedy any violation of any provision of this Exhibit and shall certify the same to the CDPH Program Contract Manager in writing.

XV.   Return or Destruction of CDPH PCI on Expiration or Termination: Upon expiration or termination of the agreement between Contractor and CDPH for any reason, Contractor shall securely return or destroy the CDPH PCI. If return or destruction is not feasible, Contractor shall provide a written explanation to the CDPH Program Contract Manager, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XI(F), above.

A.   Retention Required by Law: If required by state or federal law, Contractor may retain, after expiration or termination, CDPH PCI for the time specified as necessary to comply with the law.

B.   Obligations Continue Until Return or Destruction: Contractor's obligations under this Exhibit shall continue until Contractor returns or destroys the CDPH PCI or returns the CDPH PCI to CDPH; provided however, that on expiration or termination of the agreement between Contractor and CDPH, Contractor shall not further use or disclose the CDPH PCI except as required by state or federal law.

C.   Notification of Election to Destroy CDPH PCI: If Contractor elects to destroy the CDPH PCI, Contractor shall certify in writing, to the CDPH Program Contract Manager, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in

Section XI(F), above, that the CDPH PCI has been securely destroyed. The notice shall include the date and type of destruction method used.

XVI. Amendment: The parties acknowledge that federal and state laws regarding information security and privacy rapidly evolves and that amendment of this Exhibit may be required to provide for procedures to ensure compliance with such laws. The parties specifically agree to take such action as is necessary to implement new standards and requirements imposed by regulations and other applicable laws relating to the security or privacy of CDPH PCI. The parties agree to promptly enter into negotiations concerning an amendment to this Exhibit consistent with new standards and requirements imposed by applicable laws and regulations.

XVII. Assistance in Litigation or Administrative Proceedings: Contractor shall make itself and any subcontractors, workforce employees or agents assisting Contractor in the performance of its obligations under the agreement between Contractor and CDPH, available to CDPH at no cost to CDPH to testify as witnesses, in the event of litigation or administrative proceedings being commenced against CDPH, its director, officers or employees based upon claimed violation of laws relating to security and privacy, which involves inactions or actions by the Contractor, except where Contractor or its subcontractor, workforce employee or agent is a named adverse party.

XVIII. No Third-Party Beneficiaries: Nothing express or implied in the terms and conditions of this Exhibit is intended to confer, nor shall anything herein confer, upon any person other than CDPH or Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

XIX. Interpretation: The terms and conditions in this Exhibit shall be interpreted as broadly as necessary to implement and comply with regulations and applicable State laws. The parties agree that any ambiguity in the terms and conditions of this Exhibit shall be resolved in favor of a meaning that complies and is consistent with federal and state laws and regulations.

XX. Survival: If Contractor does not return or destroy the CDPH PCI upon the completion or termination of the Agreement, the respective rights and obligations of Contractor under Sections VI, VII and XI of this Exhibit shall survive the completion or termination of the agreement between Contractor and CDPH.

Attachment 1
Contractor Data Security Standards

1. General Security Controls

A. ***Confidentiality Statement.*** All persons that will be working with CDPH PCI must sign a confidentiality statement. The statement must include 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 PCI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for CDPH inspection for a period of three (3) years following contract termination.

B. ***Background check.*** Before a member of the Contractor's workforce may access CDPH PCI, Contractor must conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk for theft of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

C. ***Workstation/Laptop encryption.*** All workstations and laptops that process and/or store CDPH PCI must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. The encryption solution must be full disk unless approved by the CDPH Information Security Office.

D. ***Server Security.*** Servers containing unencrypted CDPH PCI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

E. ***Minimum Necessary.*** Only the minimum necessary amount of CDPH PCI required to perform necessary business functions may be copied, downloaded, or exported.

F. ***Removable media devices.*** All electronic files that contain CDPH PCI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smart devices tapes etc.). PCI must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher

G. ***Antivirus software.*** All workstations, laptops and other systems that process and/or store CDPH PCI must install and actively use a comprehensive anti-virus software solution with automatic updates scheduled at least daily.

H. ***Patch Management.*** All workstations, laptops and other systems that process and/or store CDPH PCI must have operating system and application 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.

I. ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing CDPH PCI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Must be at least eight characters. Must be a non-dictionary word. Must not be stored in readable format on the computer. Must be changed every 60 days. Must be changed 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)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation symbols)

J. ***Data Sanitization.*** All CDPH PCI must be sanitized using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH PCI is no longer needed.

2. **System Security Controls**

A. ***System Timeout.*** The system must provide an automatic timeout, requiring reauthentication of the user session after no more than 20 minutes of inactivity.

B. ***Warning Banners.*** All systems containing CDPH PCI must display a warning banner each time a user attempts access, stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.

C. ***System Logging.*** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for CDPH PCI, or which alters CDPH PCI. 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 This logging must be included for all user privilege levels including, but not limited to, systems administrators. If CDPH PCI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

D. ***Access Controls.*** The system must use role based access controls for all user authentications, enforcing the principle of least privilege.

E. ***Transmission encryption.*** All data transmissions of CDPH PCI outside the contractor's secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. Encryption can be end to end at the network level, or the data files containing CDPH PCI can be encrypted. This requirement pertains to any type of CDPH PCI in motion such as website access, file transfer, and E-Mail.

F. ***Intrusion Detection.*** All systems involved in accessing, holding, transporting, and protecting CDPH PCI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. **Audit Controls**

A. ***System Security Review.*** All systems processing and/or storing CDPH PCI 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 shall include vulnerability scanning tools.

B. ***Log Reviews.*** All systems processing and/or storing CDPH PCI must have a routine procedure in place to review system logs for unauthorized access.

C. **Change Control.** All systems processing and/or storing CDPH PCI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4. **Business Continuity / Disaster Recovery Controls**

A. **Disaster Recovery.** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic CDPH PCI 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 this agreement for more than 24 hours.

B. **Data Backup Plan.** Contractor must have established documented procedures to securely backup CDPH PCI to maintain retrievable exact copies of CDPH PCI. The backups shall be encrypted.The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore CDPH PCI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CDPH data.

5. **Paper Document Controls**

A. **Supervision of Data.** CDPH PCI 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 PCI 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 PCI is contained shall be escorted and CDPH PHI shall be kept out of sight while visitors are in the area.

C. **Confidential Destruction.** CDPH PCI must be disposed of through confidential means, using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH PSCI is no longer needed.

D. **Removal of Data.** CDPH PCI must not be removed from the premises of the Contractor except with express written permission of CDPH.

E. **Faxing.** Faxes containing CDPH PCI 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.

F. **Mailing.** CDPH PCI shall only be mailed using secure methods. Large volume mailings of CDPH PHI shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted with a CDPH approved solution, such as a solution using a vendor product specified on the CALIFORNIA STRATEGIC SOURCING INITIATIVE.

ATTACHMENT 7
ISO-SR1

CDPH
California Department of
PublicHealth

INFORMATION SECURITY OFFICE

Information Systems Security Requirements for Projects (ISO/SR1)

Version 4.0

February 2010

TABLE OF CONTENTS

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.
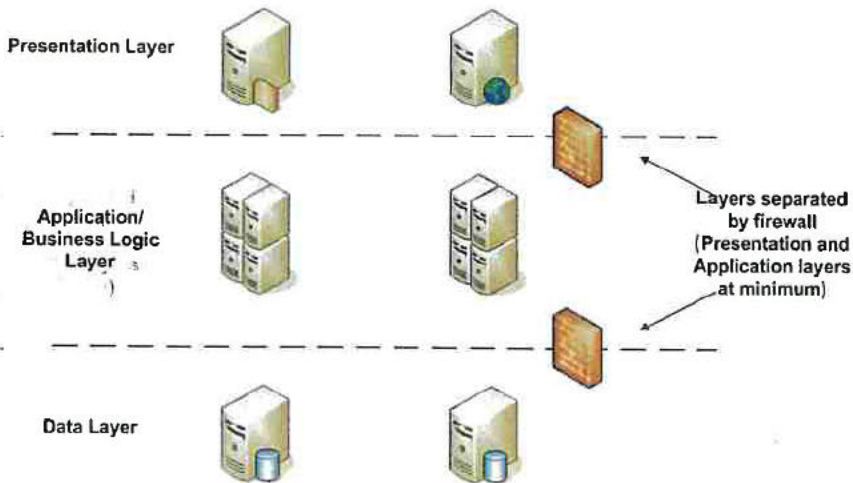
4. Input Validation

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 to 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		