SCO ID: 4265-2010921

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
20-10921	CDPH4265

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

CONTRACTING AGENCY NAME
California Department of Public Health

CONTRACTOR NAME
Deloitte Consulting LLP

2. The term of this Agreement is:

START DATE
1/29/2021

THROUGH END DATE
1/31/2022

3. The maximum amount of this Agreement is:
$2,750,132.00
Two Million Seven Hundred Fifty Thousand One Hundred Thirty Two 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
	Exhibit A	Scope of Work	2
		Attachment 1	9
	Exhibit B	Budget Detail & Provisions	3
+ -	Exhibit C	General Provisions-Information Technology DGS PD 401IT	09/5/14
+ -	Exhibit D	Special Terms & Conditions	7
+ -	Exhibit E	FEMA Provisions	5
+ -	Exhibit F	Information Privacy and Security Requirements	11
+ -	Exhibit G	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.)
Deloitte Consulting LLP

CONTRACTOR BUSINESS ADDRESS	CITY	STATE	ZIP
980 9th St #1800	Sacramento	CA	95814

PRINTED NAME OF PERSON SIGNING	TITLE
Christine Huddleson	Managing Director

CONTRACTOR AUTHORIZED SIGNATURE	DATE SIGNED
Huddleson, Christine Wight (US - Sacramento) Digitally signed by Huddleson, Christine Wight (US - Sacramento) Date: 2021.02.05 09:06:19 -08'00'	02/05/2021

SCO ID: 4265-2010921

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
20-10921	CDPH4265

STATE OF CALIFORNIA

CONTRACTING AGENCY NAME California Department of Public Health			
CONTRACTING AGENCY ADDRESS 1616 Capitol Ave	CITY Sacramento	STATE CA	ZIP 95814
PRINTED NAME OF PERSON SIGNING Amy Manasero	TITLE Assistant Branch Chief		
CONTRACTING AGENCY AUTHORIZED SIGNATURE Amy Manasero Digitally signed by Amy Manasero Date: 2021.02.05 11:51:34 -08'00'	DATE SIGNED 2/5/2021		
CALIFORNIA DEPARTMENT OF GENERAL SERVICES APPROVAL	EXEMPTION (If Applicable) PCC 1102 Executive Order N-25-20-COVID19		

Exhibit A
Scope of Work

1. Service Overview

Contractor agrees to provide to the California Department of Public Health (CDPH) the services described herein.

In response to the Governor’s Proclamation of a State of Emergency dated March 4, 2020, and Executive Order N-25-20, due to current public health emergencies, the California Department of Public Health (CDPH) has determined that CDPH must take immediate action consistent with the State’s Public Contract Code (PCC) 1102.

Please refer to Attachment 1 of this exhibit for service overview information.

2. Service Location

The services shall be performed at various locations as determined by CDPH and Contractor

3. Service Hours

The services shall be provided during various hours as determined by CDPH and Conctractor

4. Project Representatives

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

California Department of Public Health	**Deloitte Consulting LLP**
David Fisher Telephone: (916) 552-8218 Fax: N/A E-mail: David.Fisher@cdph.ca.gov	Christine Huddleson Telephone: (415) 783-2013 Fax: N/A E-mail: chuddleson@deloitte.com

B. Direct all inquiries to:

California Department of Public Health	**Deloitte Consulting LLP**
ITSD Attention: David Fisher MS 6600 1616 Capitol Ave, 73.368 Sacramento, CA 95814	Attention: Christine Huddleson 980 9th St #1800 Sacramento, CA 95814
Telephone: (916) 552-8218 Fax: N/A E-mail: David.Fisher@cdph.ca.gov	Telephone: (415) 783-2013 Fax: N/A E-mail: chuddleson@deloitte.com

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

Remittance Address

Contractor: [Deloitte Consulting

Attention “Cashier”

Exhibit A
Scope of Work

P.O. Box 844708

Dallas, TX 75284-4714
415-783-2013

chuddleson@deloitte.com

D. Either party may make changes to the information above by giving written notice to the other party. Said changes shall not require an amendment to this agreement.

5. Services to be Performed

Please refer to Attachment 1 of this Exhibit for detailed information on the services to be performed.

EXHIBIT A ATTACHMENT 1
VACCINE TRUST AND SAFETY

1. SCOPE OF WORK

To assist with the California Department of Public Health (CDPH)'s vaccine acceptance program, the Contractor will support the establishment and operation of a Trust & Safety team that will help CDPH understand and mitigate misinformation and disinformation threats to the COVID-19 vaccine rollout within the State. The Contractor will help CDPH implement a Trust & Safety effort through three core activities: 1) Trust & Safety Preparation, 2) Sensing & Analytics, and 3) Partner Engagement and Mitigation.

As part of this effort, the Contractor will rapidly assess needs, plan operations, setup tools and processes, and continually execute analysis, reporting, partner engagement and associated outreach activities. The Contractor team leaders will conduct regular and recurring planning and operational review meetings (daily engagement expected with some exceptions, specific cadence to be determined during project planning) with the CDPH team to share critical information, review project status, and address time sensitive issues.

A. TASKS

Each of the proposed tasks required to support the implementation of a Trust & Safety effort are provided in the sections below.

i. TRUST & SAFETY PREPARATION

The Contractor will conduct preparatory activities to support core Trust & Safety responsibilities, including Trust and Safety team preparations and operations management, misinformation and disinformation sensing & analytics, and partner engagement activities. This will allow the Contractor team to tailor its existing Trust & Safety blueprint to the specifics of CDPH and the vaccine acceptance program. The Contractor will leverage leading practices developed from supporting other Trust & Safety activities, as well as misinformation and disinformation activities related to vaccines performed for US Government agencies.

The Contractor team will perform the following tasks:

1. Conduct interviews with CDPH subject matter experts and review CDPH programs and documentation to become familiar with CDPH program goals, organization capabilities, privacy or security issues related to data sharing, and needs.
2. Develop an initial high-level risk assessment detailing expected and existing misinformation and disinformation threats and potential impacts with a focus on acceptance of California residents to receive the COVID-19 vaccine.
    a. Risk assessment findings will be used to inform sensing and analysis activities and refinement of CDPH Trust and Safety plans and activities.
    b. This risk assessment will include a landscape analysis of misinformation and disinformation threats that may have impact on California's acceptance of the COVID-19 vaccine.
    c. This will include information such as the type of threat, characterization of the threat, size of threats in terms of actors and audience, audience / landscape analysis, any observable trends, and key actors.
    d. The Contractor will develop a risk assessment highlighting misinformation and disinformation threats and potential impacts document for review by CDPH

3. Identify and assess internal and external stakeholders and establish lines of communications and reporting channels to set a foundation for CDPH-directed partnership engagement
4. Develop operating procedures to document and guide CDPH Trust & Safety team activities: preliminary risk assessment matrix, stakeholder engagement, information sources to be used, types of analysis and reporting, reporting cadence, and risk mitigation measures. The Contractor will provide the operating procedures document to CDPH for review and final approval.

The planning and execution of these tasks is based on the following assumptions:

1. CDPH will provide support for participating in planning meetings, interviews, and document reviews, as well as reviewing all deliverables in a timely manner.
2. Stakeholders from partner organizations will be available in a timely manner for initial planning and coordination meetings. All feedback and comments on documentation will be provided digitally within associated documents.
3. COVID-19 Vaccine Task Force Communication team responsible for vaccine communications will be available for continual meetings
4. CDPH will provide access to existing program documentation detailing goals, plans, and operations for vaccine program. Documentation and deliverables from our team and other coordination stakeholders will be made available for sharing and distribution through CDPH's preferred technology.
5. CDPH will provide access to any existing data or information associated with existing or target audiences for communication efforts related to the COVID-19 vaccine.

II. SENSING AND ANALYTICS

The Contractor will create, operate, and deliver analysis and reporting from a sensing and analytics capability. This will include identifying and employing tools and processes that the contractor's analysts will use to sense, monitor, analyze, and report on from the information environment to identify current and emerging misinformation and disinformation themes and content that may inform CDPH COVID vaccination risk mitigation decisions. The Contractor will also support the establishment of a publicly advertised email inbox within the CDPH domain to allow the public and stakeholders to provide information to CDPH on rumors related to the COVID-19 vaccine. As part of these efforts, the Contractor will help CDPH monitor developments and communications from the Centers for Disease Control and other states, and will use this information to assist CDPH with planning and communications.

The Contractor team will perform the following tasks:

1. Stand up, configure, and refine listening tools within a Contractor-hosted environment for monitoring main stream social media networks, fringe networks, news media channels and the broader information environment
2. Identify, assess and propose data collection and information gathering parameters, which include effective tracking of influencers, key words, and hashtags
3. Document rumors email inbox monitoring schedules, reporting and escalation protocols
4. Develop a COVID vaccination rumors inbox to capture rumors from partners, the public, and other stakeholders
5. Create sensing and alerting capabilities for social, fringe network, news media, and other information content to stay on top of breaking situations
6. Conduct risk analyses of content identified to triage incidents, escalate as appropriate, and develop/refine aspects of CPDH COVID vaccine risk mitigation activities

7. Develop dashboards and/or reports of varying frequency and format to inform CDPH response options, to be provided as flat-file formats such as Powerpoint, Word, Tableau stand-alone dashboards, or PDF.
8. Craft preliminary rapid response recommendations for CDPH-led mitigation activities based on information identified through Trust and Safety team activities
9. Coordinate with COVID-19 Vaccine Task Force communications team to understand the range of communication actions available to address threats.
10. Assess impacts of communications on misinformation and disinformation threats and coordinate with CDPH and communications teams on identified impacts.
11. Reports with threats and recommendations will be provided to CDPH for review.
12. Coordinate with COVID-19 Vaccine Task Force communications teams to help communicate results of reports and address feedback or questions.
13. Per guidance from CDPH, collaborate with CDPH, Governor's Office of Emergency Services, California Cybersecurity Integration Center, and State Threat Assessment Center to address other evolving threats, which may include access to sensitive information. Any additional information the contractor may obtain may be subject to non-disclosure and may require additional security clearances.
14. Collaborate with other entities as necessary, which may include other state contractors or partners (community-based organizations, vendors, etc.) to contribute to trust and safety program objectives.

The execution of these tasks is based on the following assumptions:

1. CDPH will participate in regular meetings and will review and provide timely feedback on all deliverables.
2. COVID-19 Vaccine Task Force communications teams will be available for project meetings and project communications to help coordinate on vaccine communication efforts and impacts on misinformation and disinformation threats.
3. CPDH will provide support to interpret reporting and support additional coordination and decision-making within CDPH to drive actions to address identified threats.
4. The Contractor will provide recommendations on actions to take to address threats. All specific messaging and communication will be performed by CDPH or other communication teams.
5. The Contractor will provide sensing support during normal working hours. 24/7 monitoring of threats and risks can be implemented with additional tools and personnel support, to be provided as needed.
6. The Contractor will only use publicly available social media data as part of the sensing and analysis. Information will be collated from publicly available social media sources or public / partner information provided to CDPH.
7. The contractor will use CDPH approved, contractor-provided business intelligence software and licenses to develop dashboards, which may be provided as a standalone file for viewing from desktop software. If web-based dashboards are required, the Contractor will work with CDPH to determine the most appropriate environment to host dashboards.

III. PARTNER ENGAGEMENT

The Contractor will provide advisory support to help CDPH's engagement with non-governmental, governmental, social media platform, and corporate/technology partners. These efforts will be done in concert with CDPH's communication team and broader communication goals. These efforts will help CDPH increase awareness within key communities, mitigate misinformation and disinformation threats, and amplify unified messaging and will be performed at the direction of CDPH to support the government's direct engagement with partners.

The following tasks will be performed:

1. Coordinate with CDPH to identify and prioritize new and existing partners in various sectors, including government (other state agencies, local, tribal, and federal) corporate/technology, consumer advocate, civil society, and fact check organizations
2. Conduct outreach and establish collaboration channels and processes with high-priority new and existing partners.
3. Define high-level metrics to track progress and measure ROI of partner engagement efforts.
4. Support CDPH engagement with a regular meeting cadence to provide transparency and to support contracted partners' situational awareness.
5. Support CDPH engagement with partners to facilitate continual communication channels that will help CDPH share knowledge on misinformation and disinformation threats.
6. Create and distribute tailored authoritative content to support partner efforts and/or be used to inform the public through online web posting.
7. Assess information received from partner communication channels for misinformation and disinformation threats, which will be used to guide sensing and analytics efforts above and will be included in associated reports.
8. Propose and monitor performance metrics and indicators for various communications channels to determine effectiveness of partnership engagement.

The execution of these tasks is based on the following assumptions:

1. CDPH will participate in regular meetings and will review and provide timely feedback on all deliverables.
2. CDPH will lead partner relationships, lead outreach to and follow up with stakeholders from partner organizations, will be available for meetings as needed, and will participate in regular communications through established and agreed communication channels.

In the event of any delays caused outside of the Contractors direct control, a change or deviation in scope, any failure of any stated assumptions, or the State (or its vendors) fail(s) to meet its obligations, the Contractor's ability to perform as set forth herein may be adversely impacted. An equitable adjustment to scope, cost and schedule will be agreed to by the parties in a change order to account for the impact.

B. PROPOSED STAFFING AND HOURS

Our level of effort for standing up and supporting the Trust & Safety Team is based on a 12-month period of performance.

The Contractor will provide a blend of part-time leadership and Trust and Safety operations and subject matter advisors to oversee a full-time team of analysts, partnership specialists, and social media analysts. This team has experience developing and supporting related initiatives such as those at the Department of Homeland Security and Census Bureau's 2020 Decennial Trust & Safety team. Members of the Contractor team have advanced degrees, highly specialized experience in misinformation and disinformation, existing relationships with key contacts at leading technology and social platforms and companies, backgrounds in law enforcement, the U.S. national intelligence community, and broad knowledge of social media sensing technologies.

The proposed hours, rates, and price are provided below for each task, detailed by proposed project role, staff member, labor rate, estimated hours, and cost estimate. Senior management and subject matter advisors will support each task on a part-time basis. All other staff will perform work within a 45-hour work week. Considering the highly variable nature of the vaccination program and related epidemic, additional labor hours and associated costs may be expended for each task to address unanticipated needs that arise or as the volume of work increases. Any hours above 45 hours a week need CDPH Program Designee approval. These additional hours may be expended by proposed staff, or by additional resources, to be determined and approved by CDPH as needs arise.

The price for social media listening and reporting tools have also been provided for a 12-month period. Due to COVID, work will primarily be performed remotely. Resumes will be provided to CDPH for all staff for approval.

Task 1: Trust and Safety Preparation

The Trust and Safety Preparation task will be performed over the course of a 3-week period, with significant involvement from senior management and subject matter advisors to support project initiation, strategic stakeholder and partner discussions. planning of operations, and team ramp up. One senior manager and one subject matter advisor will be available to provide oversight and guidance for the Sensing and Analysis (Task 2). An additional senior manager and subject matter advisor will provide oversight and guidance for Partnership Engagement (Task 3). The remaining team members will provide full-time support to prepare for Sensing and Analysis (Task 2) and Partner Engagement (Task 3).

#	***Roles (Classification)***	**Name**	**Labor Rate***	**Estimated Hours**	**Cost Estimate**
1	Engagement Director	Dassel, Kurt	$290.35	16	**$4,645.60**
2	Partnership Engagement - IT Senior Manager	Engel, Shane	$267.12	100	**$26,712.00**
3	Sensing and Analysis - IT Senior Manager	Maloney, Joel	$267.12	100	**$26,712.00**
4	Sensing and Analysis – Subject Matter Advisor	Feinberg, Jared	$290.35	40	**$11,614.00**
5	Partnership Engagement – Subject Matter Advisor	Faught, Caroline	$290.35	40	**$11,614.00**
6	Analytics Manager	Parker, Krista	$240.79	135	**$32,506.65**
7	Analytics Senior Consultant	Nelson, Alex	$185.22	135	**$25,004.70**
8	Analytics Senior Consultant	Cain, Haley	$185.22	135	**$25,004.70**
9	IT Consultant	Lerch, Melanie	$149.05	135	**$20,121.75**
10	IT Consultant	Gonzalez, Daniel	$149.05	135	**$20,121.75**
11	IT Consultant	Eaddy, Angela	$149.05	135	**$20,121.75**
12	IT Consultant	TBD	$149.05	135	**$20,121.75**
Total Estimated Hours / Cost:				**1241**	**$244,300.65**
Annual Social Media Sensing and Reporting Software for Access to Technology and Data					**$50,000**
TOTAL COSTS FOR TASK 1: TRUST AND SAFETY PREPARATION					**$294,300.65**

Task 2: Sensing and Analytics

The Sensing and Analysis task will be performed after the 3-week Trust and Safety Preparation task is complete for the remainder of the period of performance. One senior manager and one subject matter advisor will be available to provide oversight and guidance. The task manager will provide oversee both the Sensing and Analytics and the Partner Engagement tasks full-time, with time split equally between each task. The remaining Sensing and Analysis team members will provide full-time support to perform sensing and analysis activities.

#	***Roles (Classification)***	**Name**	**Labor Rate***	**Estimated Hours**	**Cost Estimate**
1	Engagement Director	Dassel, Kurt	$290.35	88	**$25,550.80**
2	Partnership Engagement - IT Senior Manager	Engel, Shane	$267.12	190	**$50,752.80**
3	Sensing and Analysis - IT Senior Manager	Maloney, Joel	$267.12	190	**$50,752.80**
4	Sensing and Analysis – Subject Matter Advisor	Feinberg, Jared	$290.35	80	**$23,228.00**
5	Partnership Engagement – Subject Matter Advisor	Faught, Caroline	$290.35	0	**$0.00**
6	Analytics Manager	Parker, Krista	$240.79	892	**$214,784.68**
7	Analytics Senior Consultant	Nelson, Alex	$185.22	1785	**$330,617.70**
8	Analytics Senior Consultant	Cain, Haley	$185.22	0	**$0.00**
9	IT Consultant	Lerch, Melanie	$149.05	1785	**$266,054.25**
10	IT Consultant	Gonzalez, Daniel	$149.05	1785	**$266,054.25**
11	IT Consultant	Eaddy, Angela	$149.05	0	**$0.00**
12	IT Consultant	TBD	$149.05	0	**$0.00**
Total Estimated Hours / Cost:				**6795**	**$1,227,795.28**
Average Cost Per Month*					**$111,617.75**
TOTAL COSTS FOR TASK 2: SENSING AND ANALYTICS					**$1,227,795.28**

*Average cost per month is based on a 11-month period of performance for task 2 (to start after completion of Task 1). Actual costs may vary depending on needs of the given month, to be determined in coordination with CDPH

Task 3: Partnership Engagement

The Partnership Engagement task will be performed after the 3-week Trust and Safety Preparation task is complete for the remainder of the period of performance. One senior manager and one subject matter advisor will be available to provide oversight and guidance. The task manager will provide oversee both the Sensing and Analytics and the Partner Engagement tasks full-time, with time split equally between each task. The remaining Partnership Engagement team members will provide full-time support to perform partnership engagement activities.

#	*Roles (Classification)*	Name	Labor Rate*	Estimated Hours	Cost Estimate
1	Engagement Director	Dassel, Kurt	$290.35	88	**$25,550.80**
2	Partnership Engagement - IT Senior Manager	Engel, Shane	$267.12	190	**$50,752.80**
3	Sensing and Analysis - IT Senior Manager	Maloney, Joel	$267.12	190	**$50,752.80**
4	Sensing and Analysis – Subject Matter Advisor	Feinberg, Jared	$290.35	0	**$0.00**
5	Partnership Engagement – Subject Matter Advisor	Faught, Caroline	$290.35	80	**$23,228.00**
6	Analytics Manager	Parker, Krista	$240.79	893	**$215,025.47**
7	Analytics Senior Consultant	Nelson, Alex	$185.22	0	**$0.00**
8	Analytics Senior Consultant	Cain, Haley	$185.22	1785	**$330,617.70**
9	IT Consultant	Lerch, Melanie	$149.05	0	**$0.00**
10	IT Consultant	Gonzalez, Daniel	$149.05	0	**$0.00**
11	IT Consultant	Eaddy, Angela	$149.05	1785	**$266,054.25**
12	IT Consultant	TBD	$149.05	1785	**$266,054.25**
			Total Estimated Hours / Cost:	**6796**	**$1,228,036.07**
			Average Cost Per Month*		**$111,639.64**
			TOTAL COSTS FOR TASK 3: PARTNERSHIP ENGAGEMENT		**$1,228,036.07**

*Average cost per month is based on a 11-month period of performance for task 3 (to start after completion of Task 1). Actual costs may vary depending on needs of the given month, to be determined in coordination with CDPH

Total Proposed Staffing and Hours

Task	Estimated Hours	Labor Cost Estimate	Other Costs	Total Cost Estimate
Task 1: Trust and Safety Preparation	1241	$244,300.65	$50,000.00	**$244,300.65**
Task 2: Sensing and Analytics	6795	$1,227,795.28	$0.00	**$1,227,795.28**
Task 3: Partnership Engagement	6796	$1,228,036.07	$0.00	**$1,228,036.07**
TOTAL	**14832**	**$2,700,132.00**	**$50,000.00**	**$2,750,132.00**

2. PAYMENT SCHEDULE

Invoices will be delivered on a monthly on a time and materials basis for all work performed during the given period. Invoices will be provided according to the following:

- Invoiced hourly rate aligns with contract.
- Invoiced costs do not exceed Total Estimated Costs for this WOA.
- Staff timesheets provided match actual days and hours worked

3. ONBOARDING SCHEDULE

The Contractor will provide all proposed key management and senior staff on the project start date, assumed as January 29th, 2021. These staff will support initial onboarding, planning, and project preparation during the first week. All additional junior staff will be available one week after project start to support further planning and start executing propose activities. The proposed staff and onboarding dates have been provided in the table below.

Labor Categories	**Name**	*Onboarding Date*
Engagement Director	Dassel, Kurt	Project Start Date
IT Senior Manager	Engel, Shane	
IT Senior Manager	Maloney, Joel	Project Start Date
Disease Surveillance – Subject Matter Advisor	Feinberg, Jared	Project Start Date
Disease Surveillance – Subject Matter Advisor	Faught, Caroline	Project Start Date
Analytics Manager	Parker, Krista	Project Start Date
Analytics Senior Consultant	Nelson, Alex	Project Start Date
Analytics Senior Consultant	Cain, Haley	Part-time on Project Start Date; Full-time on Project Start Date + 1 Weeks (5 Business Days)
IT Consultant	Lerch, Melanie	Project Start Date
IT Consultant	Gonzalez, Daniel	Project Start Date
IT Consultant	Eaddy, Angela	Project Start Date
IT Consultant	TBD	Project Start Date

Changes to this project start date may affect staff availability and proposed onboarding dates.

4. INITIAL SCHEUDULE OF DELIVERABLES

To support a successful on boarding, the following outlines initial expectations to have the Trust and Safety program operational in 14 calendar days.

Week Of	Key Tasks	Key Meetings
February 1	- Provide list of key questions for onboarding to determine appropriate staff for subject matter expert interviews. - Conduct initial onboarding subject matter interviews. - Provide proposed schedule for 14-day onboarding process that	- TBD: Introduction with CalOES, CalSIC, STAC.

	contemplates 24-hour review/approval periods. - Organize initial meetings with high priority social media platforms.	
February 8	- Continue to conduct onboarding subject matter interviews. - Continue to organize meetings with high priority social media platforms. - Deliver draft standard operating procedure concepts by Feb 10th. - Deliver preliminary risk assessment as outline in objective 1. - Deliver first round of reporting in draft format.	- Feb 8: onboarding with GO, HHS, CDPH executives. - Feb 10: presentation to CBO partners to include threat assessment summary, threat assessment matrix and instructions for rumors inbox.
February 15	- Continue to organize meetings with high priority social media platforms. - Deliver first round of reporting in final format. - Deliver updated standard operating procedure concepts	

5. REPORTS

The Contractor will provide the CDPH Project Representative, or their designee, with a report of activity under this contract on a bi-weekly basis. It is anticipated that these reports will commence on February 22, 2021. However, that date may change based upon project needs and as agreed upon between the Contractor and CDPH. The Contractor and CDPH Project Representative shall agree upon all final format and content requirements of activity reports in writing via e-mail.

Exhibit B
Budget Detail and Payment 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 actual expenditures incurred in accordance with the amounts shown in Exhibit A Attachment 1.

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

Wilson Yee
California Department of Public Health
ITSD
1616 Capitol Ave, 74.3.184
Sacramento, CA 95814

D. Invoice shall:

1) Be prepared on Contractor letterhead. If invoices are not on produced letterhead invoices must be signed by an authorized official, employee or agent certifying that the expenditures claimed represent activities performed and are in accordance with Exhibit A.
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: $2,750,132.00

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.

Exhibit B
Budget Detail and Payment Provisions

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.

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.

Exhibit B

Budget Detail and Payment Provisions

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.

Exhibit D
Special Terms and Conditions [Rev 06-2019]

(Applicable to consultant and personal service contracts)

The provisions herein apply to this Agreement unless the provisions are removed by reference, or superseded by an alternate provision appearing in Exhibit E of this Agreement.

Index

1. Cancellation
2. Intellectual Property Rights
3. Confidentiality of Information
4. Dispute Resolution Process
5. Excise Taxes

Exhibit D
Special Terms and Conditions

1. **Cancellation**

   A. This agreement may be cancelled by CDPH **without cause** upon 30 calendar days advancewritten notice to the Contractor.

   B. CDPH reserves the right to cancel or terminate this agreement for cause upon ten (10) business days' prior written notice if not cured within such period. The Contractor may submit a written request to terminate this agreement only if CDPH substantially fails to perform its responsibilities as provided herein.

   C. The term "for cause" shall mean that the Contractor fails to meet the terms, conditions, and/or responsibilities of this agreement.

   D. Agreement cancellation or termination shall be effective as of the date indicated in CDPH's notification to the Contractor. The notice shall stipulate any final performance, invoicing or payment requirements.

   E. Upon receipt of a notice of cancellation or termination, the Contractor shall take immediate steps to stop performance and to cancel or reduce subsequent agreement costs.

   F. In the event of early cancellation or termination, the Contractor shall be entitled to compensation for services performed satisfactorily under this agreement and expenses incurred up to the date of cancellation and any non-cancelable obligations incurred in support of this agreement.

2. **Intellectual Property Rights**

   A. **Ownership**

      1) Except where CDPH has agreed in a signed writing to accept a license, CDPH shall be and remain, without additional compensation, the sole owner of any and all rights, title and interest in all Intellectual Property, from the moment of creation, whether or not jointly conceived, that are made or conceived, by Contractor for delivery to CDPH hereunder ("work product") or by CDPH and which result directly or indirectly from this Agreement.

      2) For the purposes of this Agreement, Intellectual Property means recognized protectable rights and interest such as: patents, (whether or not issued) copyrights, trademarks, service marks, applications for any of the foregoing, inventions, trade secrets, trade dress, logos, insignia, color combinations, slogans, moral rights, right of publicity, author's rights, contract and licensing rights, works, mask works, industrial

design rights, rights of priority, know how, design flows, methodologies, devices, business processes, developments, innovations, good will and all other legal rights protecting intangible proprietary information as may exist now and/or here after come into existence, and all renewals and extensions, regardless of whether those rights arise under the laws of the United States, or any other state, country or jurisdiction.

3) For the purposes of the definition of Intellectual Property, “works” means all literary works, writings and printed matter including the medium by which they are recorded or reproduced, photographs, art work, pictorial and graphic representations and works of a similar nature, film, motion pictures, digital images, animation cells, and other audiovisual works including positives and negatives thereof, sound recordings, tapes, educational materials, interactive videos and any other materials or products created, produced, conceptualized and fixed in a tangible medium of expression. It includes preliminary and final products and any materials and information developed for the purposes of producing those final products. Works does not include articles submitted to peer review or reference journals or independent research projects.

4) In the performance of this Agreement, Contractor will exercise and utilize certain of its Intellectual Property in existence prior to the effective date of this Agreement. In addition, under this Agreement, Contractor may access and utilize certain of CDPH’s Intellectual Property in existence prior to the effective date of this Agreement. Except as otherwise set forth herein, Contractor shall not use any of CDPH’s Intellectual Property now existing or hereafter existing for any purposes without the prior written permission of CDPH. **Except as otherwise set forth herein, neither the Contractor nor CDPH shall give any ownership interest in or rights to its Intellectual Property to the other Party.** If during the term of this Agreement, Contractor accesses any third-party Intellectual Property that is licensed to CDPH, Contractor agrees to abide by all license and confidentiality restrictions applicable to CDPH in the third-party’s license agreement.

5) Contractor agrees to cooperate with CDPH in establishing or maintaining CDPH’s exclusive rights in the Intellectual Property, and in assuring CDPH’s sole rights against third parties with respect to the Intellectual Property. If the Contractor enters into any agreements or subcontracts with other parties in order to perform this Agreement, Contractor shall require the terms of the Agreement(s) to include all Intellectual Property provisions. Such terms must include, but are not limited to, the subcontractor assigning and agreeing to assign to CDPH all rights, title and interest in Intellectual Property in work product made, conceived, derived from, or reduced to practice by the subcontractor, Contractor or CDPH and which result directly or indirectly from this Agreement or any

subcontract.

6) Contractor further agrees to assist and cooperate with CDPH in all reasonable respects, and execute all documents and and take all further acts reasonably necessary to acquire, transfer, maintain, and enforce CDPH's Intellectual Property rights and interests.

B. **Retained Rights / License Rights**

1) Except for Intellectual Property in work product made, conceived, derived from, or reduced to practice by Contractor or CDPH and which result directly or indirectly from this Agreement, Contractor shall retain title to all of its Intellectual Property to the extent such Intellectual Property is in existence prior to the effective date of this Agreement or is created independently of this Agreement, and all modifications and derivatives thereof. Contractor hereby grants to CDPH, without additional compensation, a permanent, non-exclusive, royalty free, paid-up, worldwide, irrevocable, perpetual, non-terminable license to use, reproduce, manufacture, sell, offer to sell, import, export, modify, publicly and privately display/perform, distribute, and dispose Contractor's Intellectual Property with the right to sublicense through multiple layers, for any purpose whatsoever, to the extent it is incorporated in the Intellectual Property in the work product resulting from this Agreement, unless Contractor assigns all rights, title and interest in the Intellectual Property as set forth herein.

2) Nothing in this provision shall restrict, limit, or otherwise prevent Contractor from using any ideas, concepts, know-how, methodology or techniques related to its performance under this Agreement, provided that Contractor's use does not infringe the patent, copyright, trademark rights, license or other Intellectual Property rights of CDPH or third party, or result in a breach or default of any provisions of this Exhibit or result in a breach of any provisions of law relating to confidentiality.

C. **Copyright**

1) Contractor agrees that for purposes of copyright law, except for Contractor Intellectual Property contained therein, all work products [as defined in Section a, subparagraph (2)(A)] of authorship made by or on behalf of Contractor in connection with Contractor's performance of this Agreement shall be deemed "works made for hire". Contractor further agrees that the work of each person utilized by Contractor in connection with the performance of this Agreement will be a "work made for hire," whether that person is an employee of Contractor or that person has entered into an agreement with Contractor to perform the work. Contractor shall enter into a written agreement with any such person that: (i) all work performed for Contractor shall be deemed a "work made for hire"

under the Copyright Act and (ii) that person shall assign all right, title, and interest to CDPH to any work product made, conceived, derived from, or reduced to practice by Contractor or CDPH and which result directly or indirectly from this Agreement.

2) All work product, including, but not limited to, visual works or text, reproduced or distributed pursuant to this Agreement that include Intellectual Property made, conceived, derived from, or reduced to practice by Contractor or CDPH and which result directly or indirectly from this Agreement, shall include CDPH's notice of copyright, which shall read in 3mm or larger typeface: "© *[Enter Current Year e.g., 2007, etc.]*, California Department of Public Health. This material may not be reproduced or disseminated without prior written permission from the California Department of Public Health." This notice should be placed prominently on the materials and set apart from other matter on the page where it appears. Audio productions shall contain a similar audio notice of copyright.

D. **Patent Rights**

With respect to inventions made by Contractor in the performance of this Agreement, which did not result from research and development specifically included in the Agreement's scope of work, Contractor hereby grants to CDPH a license as described under Paragraph b of this provision for devices or material incorporating, or made through the use of such inventions. If such inventions result from research and development work specifically included within the Agreement's scope of work, then Contractor agrees to assign to CDPH, without additional compensation, all its right, title and interest in and to such inventions and to assist CDPH in securing United States and foreign patents with respect thereto.

E. **Third-Party Intellectual Property**

Except as provided herein, Contractor agrees that its performance of this Agreement shall not be dependent upon or include any Intellectual Property of Contractor or third party without granting to or obtaining for CDPH, without additional compensation, a license, as described in Paragraph b of this provision, for any of Contractor's or third- party's Intellectual Property in existence prior to the effective date of this Agreement. If such a license upon these terms is unattainable, and CDPH determines that the Intellectual Property should be included in or is required for Contractor's performance of this Agreement, Contractor shall obtain a license under terms acceptable to CDPH.

F. **Warranties**

1) Contractor represents and warrants that:

a. It is free to enter into and fully perform this Agreement.

b. It has secured and will secure all rights and licenses necessary for its performance of this Agreement.

c. Neither Contractor’s performance of this Agreement, nor the exercise by either Party of the rights granted in this Agreement, nor any use, reproduction, manufacture, sale, offer to sell, import, export, modification, public and private display/performance, distribution, and disposition of the Intellectual Property made, conceived, derived from, or reduced to practice by Contractor or CDPH and which result directly or indirectly from this Agreement will infringe upon or violate any Intellectual Property right, non-disclosure obligation, or other proprietary right or interest of any third-party or entity now existing under the laws of, or hereafter existing or issued by, any state, the United States, or any foreign country. There is currently no actual or threatened claim by any such third party based on an alleged violation of any such right by Contractor.

d. Neither Contractor’s performance nor any part of its performance will violate the right of privacy of, or constitute a libel or slander against any person or entity.

e. It has secured and will secure all rights and licenses necessary for Intellectual Property including, but not limited to, consents, waivers or releases from all authors of music or performances used, and talent (radio, television and motion picture talent), owners of any interest in and to real estate, sites, locations, property or props that may be used or shown.

f. It has not granted and shall not grant to any person or entity any right that would or might derogate, encumber, or interfere with any of the rights granted to CDPH in this Agreement.

g. It has appropriate systems and controls in place to ensure that state funds will not be used in the performance of this Agreement for the acquisition, operation or maintenance of computer software in violation of copyright laws.

h. It has no knowledge of any outstanding claims, licenses or other charges, liens, or encumbrances of any kind or nature whatsoever that could affect in any way Contractor’s performance of this Agreement.

2) CDPH MAKES NO WARRANTY THAT THE INTELLECTUAL PROPERTY RESULTING FROM THIS AGREEMENT DOES NOT INFRINGE UPON ANY PATENT, TRADEMARK, COPYRIGHT OR THE LIKE, NOW EXISTING OR SUBSEQUENTLY ISSUED.

G. **Intellectual Property Indemnity**

1) Contractor shall indemnify, defend and hold harmless CDPH and its assignees, and its officers, directors, employees, agents, and

successors, ("Indemnitees") from and against all claims, actions, damages, losses, liabilities (or actions or proceedings with respect to any thereof), whether or not rightful, arising from any and all actions or claims by any third party or expenses related thereto (including, but not limited to, all legal expenses, court costs, and attorney's fees incurred in investigating, preparing, serving as a witness in, or defending against, any such claim, action, or proceeding, commenced or threatened) to which any of the Indemnitees may be subject, whether or not Contractor is a party to any pending or threatened litigation, which arise out of (i) the incorrectness or breach of any of the representations, warranties, covenants or agreements of Contractor pertaining to Intellectual Property as set forth in this Section 2; or (ii) any Intellectual Property infringement, or any other type of actual or alleged infringement claim, arising out of CDPH's use, reproduction, manufacture, sale, offer to sell, distribution, import, export, modification, public and private performance/display, license, and disposition of the Intellectual Property in the work product made, conceived, derived from, or reduced to practice by Contractor or CDPH and which result directly or indirectly from this Agreement, except to the extent that such infringement arises from, or could have been avoided except for (i) the indemnified party's modification of such work product or use thereof in a manner not contemplated by this Agreement, or (ii) the failure of the indemnified party to use any corrections or modifications made available by Contractor at no additional cost. This indemnity obligation shall apply irrespective of whether the infringement claim is based on a patent, trademark or copyright registration that issued after the effective date of this Agreement. CDPH reserves the right to participate in and/or control, at Contractor's expense, any such infringement action brought against CDPH.

2) Should any Intellectual Property licensed by the Contractor to CDPH under this Agreement become the subject of an Intellectual Property infringement claim, Contractor will exercise its authority reasonably and in good faith to preserve CDPH's right to use the licensed Intellectual Property in accordance with this Agreement at no expense to CDPH. CDPH shall have the right to monitor and appear through its own counsel (at Contractor's expense) in any such claim or action. In the defense or settlement of the claim, Contractor may obtain the right for CDPH to continue using the licensed Intellectual Property; or, replace or modify the licensed Intellectual Property so that the

replaced or modified Intellectual Property becomes non-infringing provided that such replacement or modification is functionally equivalent to the original licensed Intellectual Property. If such remedies are not reasonably available, CDPH shall be entitled to a refund of all monies paid under this Agreement without restriction or limitation of any other rights and remedies available at law or in equity.

Exhibit D
Special Terms and Conditions

3) Contractor agrees that damages alone may be inadequate to compensate CDPH for breach of any term of this Intellectual Property Exhibit by Contractor. Contractor acknowledges CDPH may suffer irreparable harm in the event of such breach and agrees CDPH shall be entitled to seek to obtain equitable relief, including without limitation an injunction, from a court of competent jurisdiction, without restriction or limitation of any other rights and remedies available at law or in equity.

H. **Federal Funding**

In any agreement funded in whole or in part by the federal government, CDPH may acquire and maintain the Intellectual Property rights, title, and ownership, which results directly or indirectly from the Agreement; except as provided in 37 Code of Federal Regulations part 401.14; however, the federal government shall have a non-exclusive, nontransferable, irrevocable, paid-up license throughout the world to use, duplicate, or dispose of such Intellectual Property throughout the world in any manner for governmental purposes and to have and permit others to do so, to the extent required by applicable law.

I. **Survival**

The provisions set forth herein shall survive any termination or expiration of this Agreement or any project schedule.

3. **Confidentiality of Information**

A. The Contractor and its employees, agents, or subcontractors shall protect from unauthorized disclosure names and other identifying information concerning persons either receiving services pursuant to this Agreement or persons whose names or identifying information become available or are disclosed to the Contractor, its employees, agents, or subcontractors as a result of services performed under this Agreement, except for statistical information not identifying any such person.

B. The Contractor and its employees, agents, or subcontractors shall not use such identifying information for any purpose other than carrying out the Contractor's obligations under this Agreement.

C. The Contractor and its employees, agents, or subcontractors shall promptly transmit to the CDPH Program Contract Manager all requests for disclosure of such identifying information not emanating from the client or person.

D. The Contractor shall not disclose, except as otherwise specifically permitted by this Agreement or authorized by the client, any such identifying information to anyone other than CDPH without prior written authorization from the CDPH Program Contract Manager, except if disclosure is required by State or Federal law.

E. For purposes of this provision, identity shall include, but not be limited to name or other identifying information about the individual, such as finger or voice print or a photograph, in each case that would reasonably allow for identification of such individual.

F. As deemed applicable by CDPH, this provision may be supplemented by additional terms and conditions covering personal health information (PHI) or personal, sensitive, and/or confidential information (PSCI). Said terms and conditions will be outlined in one or more exhibits that will either be attached to this Agreement or incorporated into this Agreement by reference.

4. **Dispute Resolution Process**

A Contractor grievance exists whenever there is a dispute arising from CDPH's action in the administration of an agreement. If there is a dispute or grievance between the Contractor and CDPH, the Contractor must seek resolution using the procedure outlined below.

A. The Contractor should first informally discuss the problem with the CDPH Program Contract Manager. If the problem cannot be resolved informally, the Contractor shall direct its grievance together with any evidence, in writing, to the program Branch Chief. The grievance shall state the issues in dispute, the legal authority or other basis for the Contractor's position and the remedy sought. The Branch Chief shall render a decision within ten (10) working days after receipt of the written grievance from the Contractor. The Branch Chief shall respond in writing to the Contractor indicating the decision and reasons therefore. If the Contractor disagrees with the Branch Chief's decision, the Contractor may appeal to the second level.

B. When appealing to the second level the Contractor must prepare an appeal indicating the reasons for disagreement with the Branch Chief's decision. The Contractor shall include with the appeal a copy of the Contractor's original statement of dispute along with any supporting evidence and a copy of the Branch Chief's decision. The appeal shall be addressed to the Deputy Director of the division in which the branch is organized within ten (10) working days from receipt of the Branch Chief's decision. The Deputy Director of the division in which the branch is organized or his/her designee shall meet with the Contractor to review the issues raised. A written decision signed by the Deputy Director of the division in which the branch is organized or his/her designee shall be directed to the Contractor within twenty (20) working days of receipt of the Contractor's second level appeal. The decision rendered by the Deputy Director or his/her designee shall be the final administrative determination of the Department.

Exhibit D
Special Terms and Conditions

C. Unless otherwise stipulated in writing by CDPH, all dispute, grievance and/or appeal correspondence shall be directed to the CDPH Program Contract Manager.

D. There are organizational differences within CDPH's funding programs and the management levels identified in this dispute resolution provision may not apply in every contractual situation. When a grievance is received and organizational differences exist, the Contractor shall be notified in writing by the CDPH Program Contract Manager of the level, name, and/or title of the appropriate management official that is responsible for issuing a decision at a given level.

5. **Excise Tax**

The State of California is exempt from federal excise taxes, and no payment will be made for any taxes levied on employees' wages. The State will pay for any applicable State of California or local sales or use taxes on the services rendered or equipment or parts supplied pursuant to this Agreement. California may pay any applicable sales and use tax imposed by another state.

6. **Third-Party Beneficiaries**

Nothing express or implied in the terms and conditions of this Agreement 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.

Exhibit E

FEMA PROVISIONS

1. EQUAL EMPLOYMENT OPPORTUNITY

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

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

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

B. The contractor will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

C. The contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the contractor's legal duty to furnish information.

D. The contractor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice to be provided advising the said labor union or workers' representatives of the contractor's commitments under this section, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

E. The contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

F. The contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

G. In the event of the contractor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this contract may be canceled, terminated, or suspended in whole or in part and the contractor may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

H. The contractor will include the portion of the sentence immediately preceding paragraph (1) and the provisions of paragraphs (1) through (8) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance:

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

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

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

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

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

2. CONTRACT WORK HOURS AND SAFETY STANDARDS ACT

Compliance with the Contract Work Hours and Safety Standards Act.

A. ***Overtime requirements.*** No contractor or subcontractor contracting for any part of the contract work which may require or involve the employment of laborers or mechanics shall require or permit any such laborer or mechanic in any workweek in which he or she is employed on such work to work in excess of forty hours in such workweek unless such laborer or mechanic receives compensation at a rate not less than one and one-half times the basic rate of pay for all hours worked in excess of forty hours in such workweek.

B. ***Violation; liability for unpaid wages; liquidated damages.*** In the event of any violation of the clause set forth in paragraph (b)(1) of this section the contractor and any subcontractor responsible therefor shall be liable for the unpaid wages. In addition, such contractor and subcontractor shall be liable to the United States (in the case of work done under contract for the District of Columbia or a territory, to such District or to such territory), for liquidated damages. Such liquidated damages shall be computed with respect to each individual laborer or mechanic, including watchmen and guards, employed in violation of the clause set forth in paragraph (b)(1) of this section, in the sum of $27 for each calendar day on which such individual was required or permitted to work in excess of the standard workweek of forty hours without payment of the overtime wages required by the clause set forth in paragraph (b)(1) of this section.

C. ***Withholding for unpaid wages and liquidated damages.*** The State of California shall upon its own action or upon written request of an authorized representative of the Department of Labor withhold or cause to be withheld, from any moneys payable on account of work performed by the contractor or subcontractor under any such contract or any other Federal contract with the same prime contractor, or any other federally-assisted contract subject to the Contract Work Hours and Safety Standards Act, which is held by the same prime contractor, such sums as may be determined to be necessary to satisfy any liabilities of such contractor or subcontractor for unpaid wages and liquidated damages as provided in the clause set forth in paragraph (b)(2) of this section.

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

3. CLEAN AIR ACT

A. The contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. Section 7401 et seq.

B. The contractor agrees to report each violation to the California Air Resources Board and understands and agrees that the California Air Resources Board will, in turn, report each violation as required to assure notification to the Department of Resources Recycling and Recovery, the California Governor's Office of Emergency Services, Federal Emergency Management Agency (FEMA), and the appropriate Environmental Protection Agency Regional Office.

C. The contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FEMA.

4. THE FEDERAL WATER POLLUTION CONTROL ACT

A. The contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. Sections 1251 et seq.

B. The contractor agrees to report each violation to the State Water Resources Control Board and understands and agrees that the State Water Resources Control Board will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency (FEMA), and the appropriate Environmental Protection Agency Regional Office.

C. The contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FEMA.

5. DEBARMENT AND SUSPENSION CLAUSE

A. This contract is a covered transaction for purposes of 2 C.F.R. pt. 180 and 2 C.F.R. pt. 3000. As such the contractor is required to verify that none of the contractor, its principals (defined at 2 C.F.R. § 180.995), or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935).

B. The contractor must comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.

C. This certification is a material representation of fact relied upon by the State of California. If it is later determined that the contractor did not comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, in addition to remedies available to the State of California, the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.

D. The bidderor proposer agrees to comply with the requirements of 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. The bidder or proposer further agrees to include a provision requiring such compliance in its lower tier covered transactions.

6. BYRD ANTI-LOBBYING CLAUSE

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

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

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

A. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

B. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form- LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

C. The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

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

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

____
Signature of Contractor's Authorized Official

Name and Title of Contractor's Authorized Official ______________________ Date: ______________________

7. PROCUREMENT OF RECOVERED MATERIALS

A. In the performance of this contract the Contractor shall make maximum use of products containing recovered materials that are EPA- designated items unless the product cannot be acquired-

i. Competitively within a timeframe providing for compliance with the contract performance schedule;

ii. Meeting contract performance requirements; or

iii. At a reasonable price.

B. Information about this requirement is available at EPA's Comprehensive Procurement Guidelines web site, http://www.epa.gov/cpg/. The list of EPA-designate items is available at https://www.epa.gov/smm/comprehensive-procurement-guideline- cpg-program.

C. The Contractor also agrees to comply with all other applicable requirements of Section 6002 of the Solid Waste Disposal Act.

8. ACCESS TO RECORDS

The following access to records requirements apply to this contract:

A. The Contractor agrees to provide the State of California, the FEMA Administrator, the Controller General of the United States, or any of their authorized representatives access to any books, documents, papers, and records of the Contractor which are directly pertinent to this contract for the purposes of making audits, examinations, excerpts, and transcriptions.

B. The Contractor agrees to permit any of the foregoing parties to reproduce by any means whatsoever of to copy excerpts and transcriptions as reasonably needed.

C. The contractor agrees to provide the FEMA Administrator or his authorized representative access to construction or other work sites pertaining to the work being completed under the contract.

D. In compliance with the Disaster Recovery Act of 2018, the State of California and the Contractor acknowledge and agree that no language in this contract is intended to prohibit audits or internal reviews by the FEMA Administrator or the Comptroller General of the United States.

9. DHS SEAL, LOGO, AND FLAGS

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

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

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

11. NO OBLIGATION BY FEDERAL GOVERMENT

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

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

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

Exhibit F

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. Order of Precedence: 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. Effect on lower tier transactions: 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. Definitions: For purposes of the agreement between Contractor and CDPH, including this Exhibit, the following definitions shall apply:

A. Breach:

"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. Confidential Information: "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. Disclosure: "Disclosure" means the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.

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

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

E. Personal Information: "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

Exhibit F

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

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 where 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.

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

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 numbers listed 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

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

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.

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

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

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 Enforcement: CDPH 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.

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

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.

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

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. ***Workforce Member Assessment.*** Before a member of the Contractor's workforce may access CDPH PCI, Contractor must ensure that all workforce members that will have access to CDPH PCI have been assessed to assure that there is no indication that the workforce member may present a risk to the security or integrity of CDPH PCI. Contractor shall retain each workforce member's assessment documentation, whether in physical or electronic format, 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

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

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.

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

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.

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

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.

Exhibit G

CDPH
California Department of
PublicHealth

INFORMATION SECURITY OFFICE

Information Systems Security Requirements for Projects (ISO/SR1)

Version 4.0

February 2010

TABLE OF CONTENTS

I. PURPOSE 4

II. SCOPE OF REQUIREMENTS 4

III. CONTACT 4

IV. INFORMATION SYSTEMS SECURITY REQUIREMENTS 5

A. ADMINISTRATIVE / MANAGEMENT SAFEGUARDS 5
1. *Workforce Confidentiality Statement 5*
2. *Access Authorization & Maintenance 5*
3. *Information System Activity Review 5*
4. *Periodic System Security & Log Review 5*
5. *Disaster Recovery Plan 6*
6. *Change Control 6*
7. *Supervision of Information 6*
8. *Escorting Visitors 6*

B. TECHNICAL AND OPERATIONAL SAFEGUARDS 7
1. *System Security Compliance 7*
2. *Malware Protection 7*
3. *Patch Management 7*
4. *Encrypted Electronic Transmissions 7*
5. *Encrypted Information Storage 7*
6. *Workstation / Laptop Encryption. 7*
7. *Removable Media Encryption 8*
8. *Secure Connectivity 8*
9. *Intrusion Detection and Prevention 8*
10. *Minimum Information Download 8*
11. *Information Sanitization 8*
12. *Removal of Information 8*
13. *Faxing or Mailing of Information. 9*

C. SOLUTION ARCHITECTURE 10
1. *System Security Compliance 10*
2. *Warning Banner 10*
3. *Layered Application Design 10*
4. *Input Validation 11*
5. *Data Queries 11*
6. *Username/Password Based Authentication 12*
7. *Administrative / Privileged Accounts Management 12*
8. *Service Accounts Management 13*
9. *Authentication and Authorization 13*
10. *Authentication Logging 14*
11. *Automatic System Session Expiration 14*
12. *Automatic System Lock-out and Reporting 14*
13. *Audit (Access) 14*
14. *Audit (Minimum Information) 14*
15. *Application Security Controls 15*
16. *Application Code Security 15*
17. *Strong Authentication 16*

D. DOCUMENTATION OF SOLUTION 17
1. *System Configuration 17*
2. *Information Classification 17*
3. *System Roles and Relationships 17*
4. *Audit Method Documentation 17*
5. *Retention of Documentation 17*

E. ISO NOTIFICATIONS AND APPROVALS 18

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

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

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

I. Purpose

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

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

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

II. Scope of Requirements

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

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

III. Contact

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

IV. Information Systems Security Requirements

A. Administrative / Management Safeguards

1. Workforce Confidentiality Statement

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

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

2. Access Authorization & Maintenance

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

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

3. Information System Activity Review

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

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

4. Periodic System Security & Log Review

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

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

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

5. Disaster Recovery Plan

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

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

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

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

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

6. Change Control

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

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

7. Supervision of Information

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

8. Escorting Visitors

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

B. Technical and Operational Safeguards

1. System Security Compliance

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

2. Malware Protection

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

3. Patch Management

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

4. Encrypted Electronic Transmissions

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

5. Encrypted Information Storage

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

6. Workstation / Laptop Encryption

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

7. Removable Media Encryption

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

8. Secure Connectivity

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

9. Intrusion Detection and Prevention

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

10. Minimum Information Download

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

11. Information Sanitization

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

12. Removal of Information

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

13. Faxing or Mailing of Information

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

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

C. Solution Architecture

1. System Security Compliance

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

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

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

2. Warning Banner

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

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

> ***WARNING: This is a State of California computer system that is for official use by authorized users and is subject to being monitored and/or restricted at any time. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.***
>
> ***LOG OFF IMMEDIATELY, if you do not agree to the conditions stated in this warning.***

3. Layered Application Design

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

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

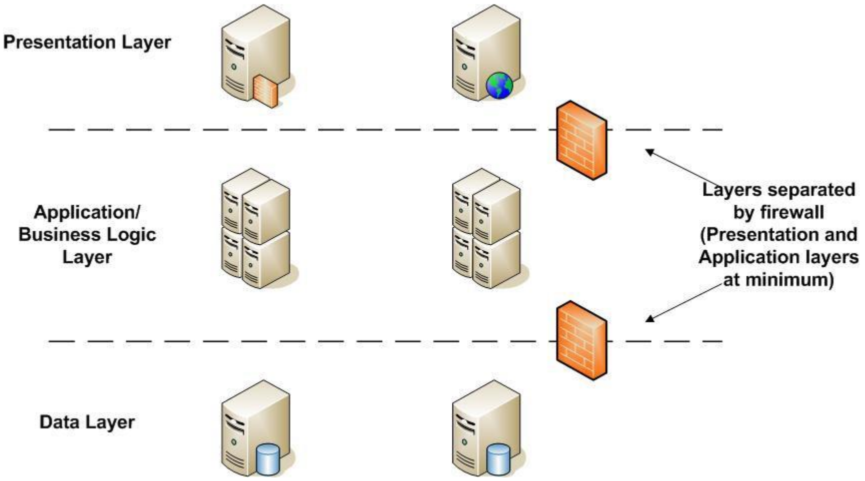
Any system request made to the Business logic layer must be authenticated.

The Data Access Logic Layer may take the form of stored procedures, database Application Programming Interface (API), Data Access Objects/Components, Data Access Middleware, Shared Data Services, or Secure Web Service. Any system request made to the Data Access logic layer must be authenticated and authorized. No direct access to the Data Persistence/Database layer will be permitted, except through the Data Access logic layer.

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

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

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


Presentation Layer
Application/ Business Logic Layer
Data Layer
Layers separated by firewall (Presentation and Application layers at minimum)

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		