

Solicitation RFP OSI 31326-

Child Welfare Services New System API Module

Solicitation Designation: Public

State of California

Solicitation RFP OSI 31326- Child Welfare Services New System API Module

Solicitation Number	RFP OSI 31326-
Solicitation Title	Child Welfare Services New System API Module
Solicitation Start Date	Dec 21, 2015 5:29:53 PM PST
Solicitation End Date	Apr 1, 2016 12:00:00 PM PDT
Question & Answer End Date	Jan 8, 2016 5:00:00 PM PST
Solicitation Contact	Phillip Sanchez Staff Information Systems Analysis 916-431-5091 phillip.sanchez@state.ca.gov
Contract Duration	90 days
Contract Renewal	Not Applicable
Prices Good for	30 days
Standard Disclaimer	<p>The State of California advises that prospective bidders periodically check the websites, including but not limited to Bidsync, and/or other state department links for modifications to bid documents. The State of California is not responsible for a prospective bidder's misunderstanding of the bid solicitation or nonresponsive bid due to failure to check these websites for updates or amendments to bid documents, and/or other information regarding the bid solicitations. Failure to periodically check these websites will be at the bidder's sole risk.</p> <p>The information published and/or responded to on these websites is public information. Confidential questions/issues/concerns should be directed to the contact on the ad.</p>
Solicitation Comments	First Release of the Child Welfare Services - New System Application Program Interface (API)

Item Response Form

Item **RFP OSI 31326--01-01 - CWS**

Quantity **1 contract**

Unit Price

Delivery Location

State of CaliforniaNo Location Specified

Qty 1

Expected Expenditure \$0.01

Description

CWS NS

IMPORTANT NOTICE TO ALL BIDDERS

Solicitation No. RFP OSI #31326 Child Welfare Services – New System Application Program Interface

This solicitation is being conducted under Public Contract Code § 12125 et seq., the Alternative Protest Process.

Submission of a proposal constitutes consent of the bidder to participate in the Alternative Protest Process.

Any protests filed in relation to the proposed Contract award shall be conducted under the procedures in this document for the Alternative Protest Process.

Any bidder wishing to protest the proposed award of this solicitation must submit a written Notice of Intent to Protest (facsimile acceptable) to the Coordinator before the close of business on the last day of the protest period, which will be established in the Notice of Intent to Award. Failure to submit a timely, written Notice of Intent to Protest waives the bidder's right to protest.

Alternative Protest Coordinator/
Department of Technology
Statewide Technology Procurement Division
10860 Gold Center Drive, Suite 200-Security
Rancho Cordova, CA 95670
MS Y12

Email: technologyprocurements@state.ca.gov

State of California
Office of Systems Integration

RFP OSI 31326
Part 1 – General Instructions
December 21, 2015



**Request for Proposal (RFP)
For
Child Welfare Services – New System (CWS-NS)
RFP OSI #31326 Application Program Interface
Final
12/21/15**

Issued by:

STATE OF CALIFORNIA
Department of Technology
Statewide Technology Procurement Division
10860 Gold Center Drive
Rancho Cordova, CA 95670

In conjunction with:

STATE OF CALIFORNIA
Office of Systems Integration
2525 Natomas Park Drive, Suite 200
Sacramento, CA 95833

Disclaimer: The original PDF version and any subsequent addendums of the solicitation released by the Procurement Official of this RFP remain the official version. In the event of any inconsistency between the Bidder's versions, articles, attachments, specifications, or provisions that constitute the Contract, the official State version of the solicitation in its entirety shall take precedence.

TABLE OF CONTENTS

1. INTRODUCTION	7
1.1 BACKGROUND.....	7
1.2 PURPOSE OF THIS REQUEST FOR PROPOSAL	7
1.3 TERM OF CONTRACT.....	9
1.4 AMERICANS WITH DISABILITIES ACT (ADA)	9
2. BIDDING INSTRUCTIONS.....	9
2.1 BIDDER ADMONISHMENT.....	9
2.2 COMMUNICATIONS AND CONTACTS	10
2.3 KEY ACTION DATES	13
2.4 RULES GOVERNING COMPETITION	14
2.5 BIDDING STEPS.....	19
2.6 PROTESTS.....	23
2.7 ALTERNATIVE PROTEST PROCESS	24
2.8 NEGOTIATIONS	25
3. ADMINISTRATIVE REQUIREMENTS	26
3.1 ABILITY TO PERFORM	26
3.2 PRIMARY BIDDER.....	27
3.3 SUBCONTRACTORS.....	27
3.4 AMENDMENT	28
3.5 FINANCIAL RESPONSIBILITY INFORMATION	28
3.6 CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY.....	29
3.8 ADMINISTRATIVE REQUIREMENTS DOCUMENT (M)	29
3.9 COVER LETTER (M).....	29
3.10 STD. 213, STANDARD AGREEMENT (M)	30
3.11 STATEMENT OF WORK (M).....	30
3.12 CONFIDENTIALITY STATEMENT (M)	31

3.13	SECRETARY OF STATE CERTIFICATION (M)	31
3.14	WORKERS COMPENSATION (M)	31
3.15	SELLER'S PERMIT (M).....	32
3.16	PAYEE DATA RECORD (STD. 204) (M)	32
3.17	IRAN CONTRACTING ACT OF 2010 (M).....	32
3.18	BIDDING PREFERENCE PROGRAMS.....	32
3.19	PRODUCTIVE USE REQUIREMENTS	36
3.20	LAWS TO BE OBSERVED.....	38
4.	BID REQUIREMENTS.....	40
4.1	QUALIFICATION REQUIREMENTS.....	40
4.2	SOLUTION REQUIREMENTS.....	43
5.	COST.....	44
6.	PROPOSAL/BID FORMAT AND SUBMISSION REQUIREMENTS	48
6.1	PREPARATION.....	48
6.2	COMPLETION OF PROPOSALS	49
6.3	DATE, TIME, AND ADDRESS OF SUBMITTALS	49
6.4	PACKAGING AND LABELING	49
6.5	FORMATTING.....	50
6.6	FINAL PROPOSAL FORMAT AND CONTENT	51
7.	EVALUATION	52
7.1	EVALUATION TEAM	53
7.2	EVALUATION STEPS	53
7.5	NEGOTIATIONS	4
8.	INFORMATIONAL ATTACHMENTS	7

State of California
Office of Systems Integration

RFP OSI 31326
Part 1 – General Instructions
December 21, 2015

RFP
PART 1
BIDDER INSTRUCTIONS

1. INTRODUCTION

This solicitation contains the instructions governing the requirements for a time and materials with a cap bid to be submitted by interested bidders. The format that bid information is to be submitted and the material to be included therein follows. This solicitation also addresses the requirements that bidders must meet to be eligible for consideration, as well as addressing bidders' responsibilities before and after award.

1.1 BACKGROUND

The Child Welfare Services (CWS) program is the primary prevention and intervention resource for child abuse and neglect in California. California is dedicated to providing a continuum of programs and services aimed at safeguarding the well-being of children and families in ways that strengthen and preserve families, encourage personal responsibility, and foster independence. The overall objective of the CWS program is that every child in California lives in a safe, stable, permanent home, nurtured by healthy families and strong communities. The CWS work does not occur in an office at a desk but in the community, homes, schools, hospitals, foster homes, and community centers.

In order to effectively protect California's at-risk children and preserve families, the State requires a multi-agency, collaborative service approach supported by a comprehensive case management system. The current Child Welfare Services/Case Management System (CWS/CMS), was a legislatively mandated statewide application implemented in 1997 based on the CWS business needs and practices at that time. Today, the CWS/CMS does not fully support child welfare practices and is no longer an economical, efficient, or effective automated tool to support the delivery of effective child welfare services.

1.2 PURPOSE OF THIS REQUEST FOR PROPOSAL

The purpose of this Request for Proposal (RFP) is to obtain the services of a qualified Bidder to provide the California Department of Social Services (CDSS) with an Application Program Interface (API) to support an overall information technology solution for the California's Child Welfare (CW) practice.

1.2.1 API Product Vision and Background

The Legacy System

The CWS/CMS is a 20 year old system with usability, maintenance, and data accuracy issues. The system was originally developed to meet the needs of users to assure the safety, permanency and well-being of children at risk of abuse, neglect or exploitation. The CWS is dedicated to modernizing and improving this business functionality. It is used by each of the 58 county child welfare and probation agencies, Title IV-E Tribes, and the State of California. Business function automation will be modernized one module at a time, with modernization including replacing and extending existing functionality.

API Module

A platform made of services, made available through modern APIs that supports agile and iterative delivery of modern [web-based] services that meets the needs of users to assure the safety, permanency and well-being of children at risk of abuse, neglect or exploitation. These high level business services are:

1. Intake/Investigations
2. Children's residential licensing
3. Case management
4. Resource management
5. Court processing
6. Eligibility
7. Financial management
8. Administration

Replacing services such as:

1. Data validation and consistency checking
2. Data access and referential integrity
3. Transaction support services
4. Logging
5. Security (authentication, access control lists and auditing)
6. Business rule enforcement that are currently implemented on a mainframe host and providing new services such as a document repository

Responses to this solicitation will be evaluated based on the bidder's total proposal in response to the requirements of this solicitation. Award, if made, will be to the single bidder awarded the highest points as calculated in accordance with the methodology defined in Section 7, EVALUATION.

1.3 TERM OF CONTRACT

Effective upon approval by the California Department of Technology, Statewide Technology Procurement Division (STPD), the term of the contract is for a three (3) month base period with three (3) additional three (3) month terms executed at the State's sole option.

1.4 AMERICANS WITH DISABILITIES ACT (ADA)

To comply with the nondiscrimination requirements of ADA, it is the policy of the State to make every effort to ensure that its programs, activities, and services are available to all persons, including persons with disabilities.

For persons with a disability needing a reasonable accommodation to participate in the procurement process, or for persons having questions regarding reasonable accommodations of the procurement process, you may contact the Procurement Official identified in subsection 2.2.1. You may also contact the State at the numbers listed below.

Important: To ensure that we can meet your need, it is best that we receive your request for reasonable accommodations at least 10 working days before the scheduled event, e.g., meeting, conference, workshop, etc., or deadline due-date for procurement documents.

The California Relay Service Telephone Numbers are:

Voice: 1-800-735-2922 or 1-888-877-5379

TTY: 1-800-735-2929 or 1-888-877-5378

Speech to Speech: 1-800-854-7784

2. BIDDING INSTRUCTIONS

2.1 BIDDER ADMONISHMENT

This procurement will follow a phased approach designed to increase the likelihood that Final Proposals will be received without disqualifying defects. The additional step(s) will (1) ensure that the bidders clearly understand the State's requirements before attempting to develop their final solutions; (2) ensure that the State clearly understands what each bidder intends to propose before those proposals are finalized; and (3) give the State and each bidder the opportunity to discuss weaknesses or potentially unacceptable elements of a bidder's proposal and give the bidder the opportunity to modify its proposal to correct such problems. Specific information regarding such steps is found in subsection 2.5, BIDDING STEPS and Section 7, EVALUATION of the solicitation.

The bidder should refer to subsection 2.5, BIDDING STEPS, to understand the phases applicable to this solicitation. It is the bidder's responsibility to:

1. Carefully read the entire solicitation.
2. Ask appropriate questions in a timely manner, if clarification is necessary.
3. Submit all required responses, by the required dates and times.
4. Make sure that all procedures and requirements of the solicitation are accurately followed and appropriately addressed.
5. Carefully re-read the entire solicitation before submitting a Draft and Final Proposal.

2.2 COMMUNICATIONS AND CONTACTS

The State uses an online procurement system known as eProcurement to communicate with perspective bidders and suppliers. Information and ongoing communications for this solicitation will be posted by the State on the eProcurement website, www.bidsync.com.

Only questions submitted in writing and answered in writing by the Procurement Official shall be binding and official. Written questions must be submitted by email to the Procurement Official identified in subsection 2.2.1, Procurement Official, using Attachment 1, Template for Question Submittal. All written questions submitted by the due date as stated in subsection 2.3, KEY ACTION DATES, will be responded to at the same time with all questions and answers posted to eProcurement in the form of a Question and Answer set.

Oral communications by Agency/state entity officers and employees concerning this solicitation shall not be binding on the State and shall in no way excuse the bidder of any obligations set forth in this solicitation.

2.2.1 Procurement Official

The Procurement Official is the State's designated authorized representative regarding this procurement.

Bidders are directed to communicate with the Procurement Official at the address below in Table 2-1: Procurement Official, to submit questions, deliver proposals, and submit all other formal correspondence regarding this procurement.

Table 2-1: Procurement Official

Hand Delivered Proposal; Parcel Post (FedEx, UPS, etc.)	United States Postal Service (USPS)
Department of Technology Statewide Technology Procurement Division Attn: Becky Fatur, Procurement Official 10860 Gold Center Drive, Suite 200 - Security Desk Rancho Cordova, CA 95670	Department of Technology Statewide Technology Procurement Division Attn: Becky Fatur, Procurement Official Mail Stop Y12 P.O. Box 1810 Rancho Cordova, CA 95741

Becky Fatur, Procurement Official
Phone: (916) 431-5558 Email: Becky.Fatur@state.ca.gov

2.2.2 Questions Regarding the Solicitation Document

Bidders requiring clarification of the intent, terms and conditions, content of this solicitation or on procedural matters regarding the competitive bid process may request clarification by submitting questions using Attachment 1, Template for Question Submittal, in an email (using the solicitation identification on the solicitation title page), to the Procurement Official listed in subsection 2.2.1. To ensure a response, questions must be received in writing by the scheduled date(s) given in subsection 2.3, KEY ACTION DATES. Question and answer sets will be provided to all bidders without identifying the submitters. At the sole discretion of the State, questions may be paraphrased by the State for clarity.

A bidder who desires clarification or further information on the content of the solicitation, but whose questions relate to the proprietary aspect of that bidder's proposal and which, if disclosed to other bidders, would expose that bidder's proposal, may submit such questions in the same manner as above, but also marked "CONFIDENTIAL," and not later than the scheduled date specified in subsection 2.3, KEY ACTION DATES to ensure a response. The bidder must explain why any questions are sensitive in nature. If the State concurs that the disclosure of the question or answer would expose the proprietary nature of the proposal, the question will be answered and both the question and answer will be kept in confidence. If the State does not concur with the proprietary aspect of the question, the question will not be answered in this manner and the bidder will be so notified.

If the bidder believes that one or more of the solicitation requirements is onerous, unfair, or imposes unnecessary constraints to the bidder in proposing less costly or alternate solutions, the bidder may request a change to the solicitation by submitting, in writing, the recommended change(s) and the facts substantiating this belief and reasons for making the recommended change using Attachment 2, Template for Request of Changes. Such request must be submitted to the Procurement Official by the date specified in subsection 2.3, KEY ACTION DATES for submitting a request for change. Oral responses shall not be binding on the State. Bidders must submit any request for changes, by the Key Action date listed in Table 2-2.

2.2.3 Intent to Bid

Bidders that want to participate in the solicitation should submit a completed Exhibit 2, Intent to Bid by the date specified in subsection 2.3, KEY ACTION DATES. This document shall be emailed to the Procurement Official identified in subsection 2.2.1. Only those bidders acknowledging interest in this solicitation will receive correspondence throughout this procurement. Correspondence to a bidder regarding this solicitation will only be given to the

bidder's designated contact person. It shall be the bidder's responsibility to immediately notify the Procurement Official identified in subsection 2.2.1, in writing, regarding any revision to the contact person information. The State shall not be responsible for proposal correspondence not received by the bidder if the bidder fails to notify the State, in writing, about any change pertaining to the designated contact person.

Bidders must notify the Procurement Official whenever their intent to bid changes or whenever there is a change in the bidder's designated contact information.

2.2.4 Bidders' Library

The Bidders' Library contains reference materials, web links, and other documents to support this RFP. The Bidder is strongly advised to review the information in the Bidders' Library. To access the Bidders' Library, the Bidder must first complete and submit Exhibit 3 Confidentiality Statement and Exhibit 23 Bidders' Library Access Authorization Form to the Procurement Official. For information on accessing the Bidders' Library, refer to the CWS-NS Bidders' Library Access and User's Guide.

Note: Items in the Bidders' Library may be updated at any time. The State is not required to issue an addendum to the RFP in order to update items in the Bidders' Library. Therefore, it is the Bidder's responsibility to regularly check the Bidders' Library for updates. Any questions concerning the Bidders' Library must be directed to the Procurement Official identified in Table 2-1, Procurement Official.

2.2.6 Cloud Computing Services

The California Department of Technology has developed a Cloud Computing Policy in order to harness the benefits of Cloud Computing. Agencies/state entities should utilize the cloud services provided through the Department of Technology, Office of Technology Services (OTech) for all new IT Projects.

California's Cloud Computing strategy is based on growing the cloud from the inside out. In support of this strategy, the Department of Technology published a Cloud Computing Reference Architecture (CCRA) in January 2014 (Provided in bidder's library). CCRA provides guidance to all Agencies/state entities to build or evaluate cloud services. Using this guidance, OTech developed a secure state government-wide private cloud, referred to as "CalCloud". CalCloud is currently operational and offers Infrastructure as a Service (IaaS) and Software as a Service for Oracle database to all Agencies and State entities. Bidders can also propose other database software that can work in CalCloud environment. Refer to SAM 4983.1 for the Cloud First policy.

Per the State's Cloud Computing Policy, OTech will host the CWS-NS on CalCloud. Bidders will be required to review the CalCloud service offerings, rates, and standards in the Bidders' Library

in order to submit a Final Proposal. It is highly recommended that if bidders have questions that they submit them no later than the respective time and date in subsection 2.3, KEY ACTION DATES for such written questions to allow the State time to address any questions the bidder may have to ensure its proposed solution is fully responsive to the requirements of this RFP.

Additional information regarding OTech service offerings and rates is provided in the Bidders' Library.

2.3 KEY ACTION DATES

Key Action Dates provided in Table 2-2: Key Action Dates contain pertinent dates and times by which actions must be taken or completed. If the State finds it necessary to change these dates or times, it will be accomplished via an addendum to this solicitation with the exception of dates listed after the Bidder's submission of Final Proposals. Dates listed after the Bidder's submission of Final Proposals are estimated and may be adjusted without addendum to this solicitation. All times listed are for Pacific Standard Time (PST).

Table 2-2: Key Action Dates

Key Action Dates		
Item	Action	Date and Time
1.	Release of Solicitation	December 21, 2015
2.	Last day to submit Exhibit 1, Intent to Bid, and Exhibit 3, signed Confidentiality Statement	January 8, 2016
3.	Last day to submit written questions using Attachment 1 and request changes to requirements using Attachment 2 ¹	January 12, 2016
4.	State's response to submitted bidder questions and request for changes	January 22, 2016
5.	Last day to protest solicitation requirements ¹	February 1, 2016
6.	Last day to submit Final Proposals ³	February 11, 2016 12:00 p.m. (PST)
7.	Evaluation Period ⁴	February 12 -22, 2016

Key Action Dates		
Item	Action	Date and Time
8.	Public Cost Opening	March 2, 2016
9.	Notification of Intent to Award	March 7, 2016
10.	Last day to protest selection ⁴	March 9, 2016
11.	Contract Award	April 1, 2016
12.	Contract Execution	TBD

¹ Or five (5) business days following the last Addendum that changes the requirements of the solicitation.

² Actual dates to be determined when the number of bidders is known.

³ All dates after submission of Final Proposals are approximate and may be adjusted as conditions indicate without addendum to this solicitation.

⁴ See subsection 2.6, PROTESTS.

⁵ Based on the number of proposals received.

2.4 RULES GOVERNING COMPETITION

This solicitation, the evaluation of responses, and the award of any resultant contract shall be made in conformance with current competitive bidding procedures as they relate to the procurement of IT Goods and Services by public bodies in the State of California.

2.4.1 Identification and Classification of Solicitation Requirements

The State has established certain requirements with respect to proposals to be submitted by prospective contractors. The use of "shall", "must," or "will" (except to indicate simple futurity) in the solicitation indicates a requirement or condition which is Mandatory. A deviation, if not material, may be waived by the State.

A deviation from a requirement is material if the response is not in substantial accord with the solicitation requirements, provides an advantage to one bidder over other bidders, or has a

potentially significant effect on the delivery, quantity, or quality of items bid¹, amount paid to the supplier, or on the cost to the State. Material deviations cannot be waived.

The words “should” or “may” in the solicitation indicate desirable attributes or conditions, but are non-Mandatory in nature. Deviation from or omission of such a desirable feature, even if material will not in itself cause rejection of the bid.

2.4.2 Solicitation Documents

This solicitation document includes, in addition to an explanation of the State’s requirements which must be met, instructions which prescribe the format and content of proposals to be submitted and the model of the contract to be executed between the State and the successful bidder.

If a bidder discovers any ambiguity, conflict, discrepancy, omission, or other error in this solicitation document, the bidder shall immediately notify the Procurement Official identified in subsection 2.2.1, of such error in writing and request clarification or modification of the document.

Modifications will be made by addenda issued pursuant to subsection 2.4.6, Addenda. Such modifications shall be given by written notice to all parties who have identified themselves as bidders to the Procurement Official without divulging the source of the request. Insofar as practicable, the State will give such notices to other interested parties, but the State shall not be responsible therefore.

If the solicitation document contains an error known to the bidder, or an error that reasonably should have been known, the bidder shall bid at its own risk. If the bidder fails to notify the State of the error prior to the date fixed for submission of proposals, and is awarded the contract, the bidder shall not be entitled to additional compensation or time by reason of the error or its later correction.

2.4.3 Examination of the Work

The bidder should carefully examine the entire solicitation document and any addenda thereto, and all related materials and data referenced in the solicitation document or otherwise available to the bidder, and should become fully aware of the nature and location of the work, the quantities of the work, and the conditions to be encountered in performing the work. Specific conditions to be examined may be listed in Section 3, ADMINISTRATIVE REQUIREMENTS and/or Section 4, BID REQUIREMENTS.

¹ The word "bid" as used throughout is intended to mean "proposed," "propose" or "proposal" as appropriate.

2.4.4 Exclusion for Conflict of Interest

No consultant shall be paid out of State funds for developing recommendations on the acquisition of information technology (IT) products or services or assisting in the preparation of the Project Approval Lifecycle documents (stages 2, 3, or 4) or feasibility study, while in effect, if that consultant is to be a source of such acquisition or could otherwise directly and/or materially benefit from State adoption of such recommendations or the course of action recommended in the Project Approval Lifecycle documents (stages 2, 3, or 4) or feasibility study. Further, no consultant shall be paid out of State funds for developing recommendations on the disposal of State surplus IT products, if that consultant would directly and/or materially benefit from State adoption of such recommendations.

A consultant shall not be eligible to serve as the Prime Contractor or subcontractor pursuant to this solicitation if the contractor/subcontractor is currently working on the solicitation in an Independent Verification and Validation (IV & V) role.

2.4.5 Confidentiality

Bidder material becomes public only after the notice of Intent to Award is released. If material marked “confidential,” “proprietary,” or “trade secret” is requested pursuant to the Public Records Act, the State will make an independent assessment whether it is exempt from disclosure. If the State disagrees with the bidder, the State will notify the bidder and give them a reasonable opportunity to justify their position or obtain a court order protecting the material from disclosure.

Bidders should be aware that marking a document “confidential” or “proprietary” in a Final Proposal may exclude it from consideration for award and will not keep that document from being released after notice of award as part of the public record, unless a court has ordered the State not to release the document. The content of all working papers and discussions relating to the bidder’s proposal shall be held in confidence indefinitely, unless the public interest is best served by an item’s disclosure because of its direct pertinence to a decision, agreement or the evaluation of the proposal.

Any disclosure of confidential information by the bidder is a basis for rejecting the bidder’s proposal and ruling the bidder ineligible to further participate. Any disclosure of confidential information by a State employee is a basis for disciplinary action, including dismissal from State employment, as provided by Government Code §19570 et seq. Total confidentiality is paramount; it cannot be over emphasized.

2.4.6 Addenda

The State may modify the solicitation prior to the date fixed for Contract Award by issuance of an addendum to all bidders who are participating in the bidding process at the time the addendum is issued. Addenda will be numbered consecutively.

If a bidder determines that an addendum unnecessarily restricts its ability to bid, the bidder is allowed five (5) business days to submit written questions and protest the addendum according to the instructions contained in subsection 2.6.1, Requirements (Initial) Protests.

2.4.7 Bidder's Cost

Costs for developing proposals are the responsibility entirely of the bidder and shall not be chargeable to the State.

2.4.8 Discounts

In connection with any discount offered, except when a provision is made for a testing period preceding acceptance by the State, time will be computed from the date of delivery of the supplies or equipment as specified, or from date correct invoices are received in the office specified by the State if the latter date is later than the date of delivery. When a provision is made for a testing period preceding Acceptance by the State, the date of delivery shall mean the date the supplies or equipment are accepted by the State during the specified testing period. Payment is deemed made, for the purpose of earning the discount, on the date of mailing the State warrant or check.

Cash discounts offered by bidders for the prompt payment of invoices will not be considered in evaluating offers for award purposes; however, all offered discounts will be taken if the payment is made within the discount period, even though not considered in the evaluation of offers.

2.4.9 Signature of Proposal

A cover letter (which shall be considered an integral part of the Final Proposal) and Standard Agreement STD. 213, and any proposal form requiring signature, shall be signed by an individual who is authorized to bind the bidding firm contractually. The signature block must indicate the title or position that the individual holds in the firm. An unsigned Final Proposal may be rejected.

The Draft Proposal, if applicable, must also contain the cover letter and STD. 213, including the title of the person who will sign, but need not contain the signature.

2.4.10 Irrevocable Offer

A bidder's Final Proposal is an irrevocable offer for 180 days following the scheduled date for Submission specified in subsection 2.3, KEY ACTION DATES. A bidder may extend the offer in the event of a delay of contract award.

2.4.11 False or Misleading Statements

Proposals which contain false or misleading statements, or which provide references which do not support an attribute or condition claimed by the bidder, may be rejected. If, in the opinion of the State, such information was intended to mislead the State in its evaluation of the proposal, and the attribute, condition, or capability is a requirement of this solicitation document, it will be the basis for rejection of the proposal.

2.4.12 Joint Bids (Not Applicable)

A joint proposal [two (2) or more bidders quoting jointly on one (1) bid] may be submitted and each participating bidder must sign the joint bid. If the contract is awarded to joint bidders, it shall be one indivisible contract. Each joint contractor will be jointly and severally responsible for the performance of the entire contract, and the joint bidders must designate, in writing, one individual having authority to represent them in all matters relating to the contract. The State assumes no responsibility or obligation for the division of orders or purchases among joint contractors.

2.4.13 Unfair Practices Act and Other Laws

Bidder warrants that its proposal complies with the Unfair Practices Act (Business and Professions Code §17000 et seq.) and all applicable State and Federal laws and regulations.

2.4.14 Fair Employment and Housing Commission Regulations

The California Government Code §12990 requires all State contractors to have implemented a Nondiscrimination Program before entering into any contract with the State. The Department of Fair Employment and Housing (DFEH) randomly selects and reviews State contractors to ensure their compliance with the law. DFEH periodically disseminates a list of contractors who have not complied. Any contractor so identified is ineligible to enter into any State contract.

2.4.15 Plastic Trash Bag Certification Violations

Public Resources Code §42290 et seq. prohibits the State from contracting with any supplier, manufacturer, or wholesaler, and any of its divisions, subsidiaries, or successors that have been determined to be noncompliant to the recycled content plastic trash bag certification

requirements. This includes award of a State contract or subcontract or renewal, extension, or modification of an existing contract or subcontract. Prior to award the State shall ascertain if the intended awardee or proposed subcontractor is a business identified on the current CalRecycle noncompliant list(s). In the event of any doubt of the status or identity of the business in violation, the State will notify the Board of the proposed award and afford the Board the opportunity to advise the State. No award will be made when either the bidder or a subcontractor has been identified either by published list or by advice from the Board, to be in violation of certification requirements.

2.4.16 Air or Water Pollution Violations

Unless the contract is less than \$25,000 or with a non-competitively bid contractor, Government Code §4477 prohibits the State from entering into any contract for the purchase of supplies, equipment, or services from any person, including a corporation or other business association who is in violation of any order or resolution not subject to review promulgated by the State Air Resources Board or an air pollution control district, or is subject to a cease and desist order not subject to review issued pursuant to §13301 of the Water Code for violation of waste discharge requirements or discharge prohibitions, or is finally determined to be in violation of provisions of federal law relating to air or water pollution.

2.5 BIDDING STEPS

The procurement process may require any or all of the following types of compliance phase (preliminary) proposals: Conceptual Proposal, Detailed Technical Proposal, and/or Draft Proposal. The procurement process requires a final phase consisting of a Final Proposal.

The procurement process to be used in this solicitation is composed of at least one (1) phase of proposal development. **Refer to subsection 2.3, KEY ACTION DATES to determine which phases and mandatory steps are included in this solicitation document.**

2.5.1 Compliance Phase

The Compliance Phase is an iterative, conversational mode of proposal and contract development. It requires the State, working together in confidence with each bidder, to assess and discuss the viability and effectiveness of the bidder's proposed methods of meeting the State's needs as reflected in the solicitation. It is a departure from the rigid "either accept or reject" philosophy of traditional competitive bidding, yet it is highly competitive in nature. It provides the flexibility needed for the bidder to test a solution prior to formal submittal of the Final Proposal, and it facilitates the correction of defects before they become detrimental to the bid. The compliance phase proposals or *preliminary proposals* may include the submission of a Conceptual Proposal and/or a Detailed Technical Proposal, and/or a Draft Proposal by the

bidder, Confidential Discussions of the bidder's proposal(s) and Revised Draft Proposals to address the correction of defects.

The additional Compliance Phase step(s) will (1) ensure that the bidders clearly understand the State's requirements before attempting to develop their final solutions; (2) ensure that the State clearly understands what each bidder intends to propose before those proposals are finalized; and (3) give the State and each bidder the opportunity to discuss weaknesses or potentially unacceptable elements of a bidder's proposal and give the bidder the opportunity to modify its proposal to correct such problems.

All bidders are strongly encouraged to follow the scheduled steps of this procurement document in order to increase the chance of submitting a compliant Final Proposal. **Costs submitted in any submission other than the Final Proposal may preclude the bidder from continuing in the process.**

2.5.1.1 Conceptual Proposal

The Conceptual Proposal is optional and included for the purpose of allowing each bidder to provide a general concept of a proposal. It should contain just enough detail to enable the evaluators to determine if the bidder is on the right track toward meeting the functional requirements as stated in the solicitation; and if not, where the bidder must change a concept. This step invites the bidder to be as innovative as the solicitation requirements allow in eliminating unnecessary constraints.

2.5.1.2 Detailed Technical Proposal

The Detailed Technical Proposal is optional and included for the purpose of allowing each bidder to provide a detailed technical description of its proposal. The proposal should determine whether the proposal is responsive to all the requirements of the solicitation, and if not, which elements are not responsive and what changes would be necessary.

2.5.1.3 Draft Proposal

The purpose of the Draft Proposal is to provide the State with an "almost final" proposal in order to identify any faulty Administrative, Bid Requirement or any aspects of the proposal which, if not corrected, could cause the Final Proposal to be rejected.

The Draft Proposal must be complete in every respect as required by the Section 6, PROPOSAL/BID FORMAT AND SUBMISSION REQUIREMENTS. The inclusion of cost information in the Draft Proposal may be a basis for rejecting the proposal and notifying the bidder that further participation in the procurement is prohibited.

REVIEW OF THE DRAFT PROPOSAL BY THE STATE MAY INCLUDE CONFIDENTIAL DISCUSSIONS WITH INDIVIDUAL BIDDERS AND THE STATE WILL PROVIDE FEEDBACK TO THE BIDDER PRIOR TO SUBMITTAL OF THE FINAL PROPOSAL. Regardless of the inclusion of a confidential discussion, the State will notify the bidder of any defects it has detected in the Draft Proposal, or of the fact that it did not detect any such defects. Such notification is intended to minimize the risk that the Final Proposal will be deemed defective; however, THE STATE WILL NOT PROVIDE ANY WARRANTY THAT ALL DEFECTS HAVE BEEN DETECTED AND THAT SUCH NOTIFICATION WILL NOT PRECLUDE REJECTION OF THE FINAL PROPOSAL IF SUCH DEFECTS ARE LATER FOUND.

The State's evaluation and review of preliminary proposal(s) is cursory. Therefore, bidders are cautioned not to rely on the State, during these evaluations and reviews, to discover and report to the bidders all defects and errors in the submitted documents. Before submitting each document, the bidder should carefully proof it for errors and adherence to the solicitation requirements.

2.5.1.4 Evaluation of Preliminary Proposal(s) and Discussion Agenda

The State will review each preliminary proposal including conceptual, detailed technical and draft proposals, as applicable in the solicitation. Review of the preliminary proposal(s) will be in accordance with the evaluation methodology outlined in the solicitation for the purpose of identifying areas in which the proposal is nonresponsive to a requirement, is otherwise defective, or in which additional clarification is required in order that the State may fully understand the ramifications of an action proposed by the bidder. As a result of this evaluation, the State may prepare an agenda of items to be discussed with the bidder, and will normally transmit the agenda to the bidder at least two (2) working days before the scheduled meeting. The agenda may also include, in addition to the identification of discovered defects, a discussion of the bidder's proposed supplier support, implementation plans, validation plans, demonstration plans, and proposed contracts, as appropriate.

2.5.1.5 Confidential Discussion with Each Bidder

In accordance with the discussion agenda, the State may meet with each bidder for the purpose of discussing the preliminary proposal(s) in detail. The bidder may bring to the discussion those persons who may be required to answer questions or commit to changes. As the first order of business, the bidder may be asked to give a short proposal overview presentation. To the maximum extent practical, the bidder will address the concerns of the State, as expressed in the discussion agenda, and should be prepared to answer any questions that may arise as a result of the presentation. The participants will then proceed to discuss each of the agenda items.

The State will not make counter proposals to a bidder's proposed solution to the solicitation document requirements. The State will only identify its concerns, ask for clarification, and

express its reservations if a particular requirement of the solicitation document is not, in the opinion of the State, appropriately satisfied. The primary purpose of this discussion is to ensure that the bidder's Final Proposal will be responsive.

2.5.1.6 Submission of Amended Preliminary Proposal(s)

If, at the conclusion of the Confidential Discussion, the State determines that required changes can only be fully confirmed through the submission of an amended preliminary proposal(s), the State may require the submission of an addendum to the bidder's preliminary proposal(s) consisting only of those pages which were in doubt or a complete resubmittal.

The bidder will be notified of defects discovered in these submittals as well. The State will not provide any warranty that all defects have been detected and that such notification will not preclude rejection of the Final Proposal if such defects are later found.

2.5.2 Final Phase

The purpose of the Final Phase is to obtain proposals that are responsive in every respect. The Final Proposal is a mandatory step for all bidders; all other steps are optional unless otherwise stated in subsection 2.3, KEY ACTION DATES.

2.5.2.1 Final Proposal

The Final Proposal must be complete, including all cost information, required signatures, contract changes agreed to via an addendum and corrections made to those defects noted by the State in its review of the Draft Proposal, if any. Cost data as identified in Section 6, PROPOSAL/BID FORMAT AND SUBMISSION REQUIREMENTS must be submitted under separate, sealed cover.

2.5.3 Withdrawal and Resubmission/Modification of Proposals

A bidder may withdraw its Conceptual Proposal, Detailed Technical Proposal or Draft Proposal at any time by written notification. A bidder may withdraw its Final Proposal at any time prior to the Final Proposal submission date and time specified in subsection 2.3, KEY ACTION DATES by submitting a written notification of withdrawal signed by an authorized representative of the bidder in accordance with subsection 2.4.9, Signature of Proposal. The bidder may thereafter submit a new or modified proposal prior to such proposal submission date and time.

Modification offered in any other manner, oral or written, will not be considered. Other than as allowed by law, Final Proposals cannot be changed or withdrawn after the date and time designated for receipt, except as provided in the solicitation document.

2.5.4 Disposition of proposals

All materials submitted in response to this solicitation will become the property of the State of California and will be returned only at the State's option and at the bidder's expense. At a minimum, the Master Copy of the Final Proposal shall be retained for official files and will become a public record after the Notification of Intent to Award is posted. However, materials the State considers as confidential information (such as confidential financial information submitted to show bidder responsibility) will be returned upon request of the bidder.

2.6 PROTESTS

There are two (2) types of protests: 1) requirements (initial) protests and 2) award protests. A protest shall be submitted according to the procedure below.

2.6.1 Requirements (Initial) Protests

Protests regarding any issue other than selection of the "Successful Bidder" are requirements protests. A protest of requirements is a challenge brought against a requirement that may be restrictive, ambiguous, favors a specific vendor/solution/technology, etc. Requirement Protests will be heard and resolved by the Deputy Director of the Department of Technology, Statewide Technology Procurement Division (STPD), whose decision will be final.

Before a requirements protest is submitted, the bidder must make full and timely use of the procedures described in this section to resolve any outstanding issue(s) between the bidder and the State. The procurement procedure is designed to give the bidder and the State adequate opportunity to submit questions and discuss the requirements, proposals and counter proposals before the Final Proposal is due. The protest procedure is made available in the event that a bidder cannot reach a fair agreement with the State after exhausting these procedures.

All protests of requirements must be made in writing, signed by an individual authorized under subsection 2.4.9, Signature of Proposal, and contain a statement of the reason(s) for protest, citing the law, rule, regulation, or procedures on which the protest is based. The protestant must provide facts and evidence to support the claim. All protests to the solicitation requirements must be received by the Deputy Director of the Department of Technology Statewide Technology Procurement Division (STPD) as promptly as possible, but not later than the respective time and date in subsection 2.3, KEY ACTION DATES for such protests. Protests must be mailed or hand delivered to:

Table 2-3: Protest Delivery Information

Street Address:	Mailing Address:
Marnell Voss, Deputy Director Department of Technology Statewide Technology Procurement Division 10860 Gold Center Drive, 4 th Floor Rancho Cordova, CA 95670	Marnell Voss, Deputy Director Department of Technology Statewide Technology Procurement Division P.O. Box 1810 MS Y12 Rancho Cordova, CA 95741-1810

Copies of all protests are to be sent to the Procurement Official listed in subsection 2.2.1.

2.6.2 Award Protest

An award protest is where a bidder has submitted a final proposal which it believes to be responsive to the requirements of the solicitation document and to be the proposal that should have been selected according to the evaluation procedure in Section 7, EVALUATION and the bidder believes the State has incorrectly selected another bidder for award.

2.7 ALTERNATIVE PROTEST PROCESS

This procurement is being conducted under the provisions of the Alternative Protest Process (Public Contract Code § 12125 et seq.). Bidder understands that by submitting a proposal to this procurement, the bidder consents to participation in the Alternative Protest Process, and agrees that all protests of the proposed award shall be resolved by binding arbitration pursuant to the California Code of Regulations, Title 1, Division 2, Chapter 5.

<http://www.dgs.ca.gov/oah/GeneralJurisdiction/BidProtestRegs.aspx>

A Notice of Intent to Award for this solicitation will be publicly posted on the 2nd floor Security Desk of the Department of Technology, 10860 Gold Center Drive, Rancho Cordova, CA and sent via email to any bidder who submits a written request for notice and provided an email address.

During the protest period, any bidder who submitted a final proposal may protest the proposed award on the following grounds:

1. For major information technology acquisitions – that there was a violation of the solicitation procedure(s) and that the protesting bidder's proposal should have been selected; or
2. For any other acquisition – that the protesting bidder's proposal should have been selected in accordance with the selection criteria in the solicitation document.

A written Notice of Intent to Protest the proposed award of this solicitation must be received (email or facsimile acceptable) by the Coordinator by the date and time specified in subsection

2.3, KEY ACTION DATES. Failure to submit a timely, written Notice of Intent to Protest waives bidder's right to protest.

Bidder is to send the Notice of Intent to Protest to:

Table 2-4: Notice of Intent to Protest Address

Hand Delivered Bid; Parcel Post (FedEx, UPS, etc.)	United States Postal Service (USPS)
Department of Technology Statewide Technology Procurement Division Attn: Alternative Protest Process Coordinator 10860 Gold Center Drive, Suite 200 – Security Desk Rancho Cordova, CA 95670	Department of Technology Statewide Technology Procurement Division Attn: Alternative Protest Process Coordinator Mail Stop Y12 P.O. Box 1810 Rancho Cordova, CA 95741-1810
Fax: (916) 463-9910 Email: technologyprocurements@state.ca.gov	

Copies of the protest are to be sent to the Procurement Official listed in subsection 2.2.1.

Within two (2) working days after the last day to submit a Notice of Intent to Protest, the Coordinator must receive from the protesting bidder the complete protest filing including the signed, written detailed statement of protest including exhibits, filing fee and deposit or small business certification as applicable. Untimely submission of the complete protest filing waives the bidder's right to protest.

Protest bond requirement: the bond amount for this Alternative Protest Process shall not be less than Ten percent (10%) of the estimated contract value. See California Code of Regulations, Title 1, §1418.

Refer to Attachment 3, Procedure for conducting protests under Alternative Protest Process.

2.8 NEGOTIATIONS

The State of California reserves the right to negotiate. Should it be determined that it is in the State's best interest, the State will conduct negotiations under PCC §6611. The purpose of the Negotiation Process is to maximize the State's ability to obtain a best value solution, based on the requirements and the evaluation factors set forth in the solicitation.

3. ADMINISTRATIVE REQUIREMENTS

This Section 3 contains the Mandatory Administrative Requirements that must be met in order to be considered responsive to this solicitation. Unless designated otherwise, all of the requirements in this section are mandatory. However, documents that must be submitted with the bidder's Final Proposal are noted as Mandatory "(M)" in this section.

Additionally, this Section 3 contains Optional requirements noted as Optional "(O)" that may require documents to be submitted with bidder's proposal response. The Administrative Requirements listed in this section are denoted as follows:

1. (M) All items labeled "Mandatory" or "M" are not negotiable. To be considered responsive and responsible to these requirements, all requirements identified as (M) must be responded to. A "Fail" will result in a proposal being deemed non-responsive and, therefore, will be disqualified. Failure to respond to any mandatory requirements shall result in disqualification of the proposal. The responses will be evaluated in accordance with Section 7, EVALUATION.
2. (O) All sections labeled as "Optional" or "O" are not required to be offered by the bidder in order to be compliant to the solicitation requirements. A bidder may choose whether to meet administrative requirements labeled as (O) such as those relating to preference points. However, if a bidder offers any of these (O) requirements, the bidder must meet the minimum requirements as stated in the section. The State will review responses to optional requirements and apply points, if applicable, per criteria stated in Section 7, EVALUATION.

3.1 ABILITY TO PERFORM

Prior to award of the contract, the State must be assured that the bidder selected has all of the resources to successfully perform under the contract. This includes, but is not limited to, personnel in the numbers and with the skills required; equipment of appropriate type and in sufficient quantity; financial resources sufficient to complete performance under the contract; and experience in similar endeavors. If, during the evaluation process, the State is unable to assure itself of the bidder's ability to perform under the contract, if awarded, the State has the option of requesting from the bidder any information that the State deems necessary to determine the bidder's responsibility. If such information is required, the bidder will be so notified and will be permitted five (5) State business days to submit the information requested in writing. Examples of the type of financial responsibility information requested may include annual reports and current audited balance sheets for the bidder firm.

3.2 PRIMARY BIDDER

An award, if made, will be to a Primary Bidder. The awarded Primary Bidder will be responsible for successful performance of all subcontractors and support services offered in response to this solicitation. All State policies, guidelines, and requirements that apply to the Primary Bidder also apply to subcontractors, as applicable to the products and services they provide and to their role as a subcontractor. Furthermore, the State will consider the Primary Bidder to be the sole point of contact regarding contractual matters for the term of the resulting contract. The Bidder shall not assign financial documents to a third-party without prior written approval by the State, and an amendment to the resulting contract.

3.3 SUBCONTRACTORS

It is the bidder's responsibility to ensure any subcontractor that the bidder chooses to use in fulfilling the requirements of this solicitation, which is expected to receive more than ten percent (10%) of the value of the contract, must also meet all Administrative, and Bid Requirements of the solicitation, as applicable to the services provided by the subcontractor.

Nothing contained in the resulting contract shall create any relationship between the State and any subcontractors, and no subcontract shall relieve the bidder of its responsibilities and obligations. The bidder is fully responsible to the State for the acts and omissions of its subcontractors and of persons either directly or indirectly employed by them.

The contractor shall not change subcontractor(s) and/ or DVBE subcontractor(s) if such changes conflict with the work to be performed under this contract. For DVBE subcontractor changes, the contractor shall utilize another DVBE subcontractor. The State recognizes that changes to subcontractor(s) may be necessary and in the best interests of the State, however, advance notification of a contemplated change and the reasons for such change must be made to the State no less than seven (7) business days prior to the existing subcontractor's termination. If this should occur, the contractor should be aware that the State contract administrator or designee must approve any changes to the subcontractor(s) prior to the termination of the existing subcontractor(s). This also includes any changes made between submittal of the Final Proposal and actual start of the contract.

The State will not compensate the contractor for any of the contractor's time or effort to educate or otherwise make the new subcontractor(s) ready to begin work on the contract.

The bidder's obligation to pay its subcontracts is an independent obligation from the State's obligation to pay or to enforce the payment of any money to any subcontractor. Contractor is solely responsible for any payments to or claims made by subcontractors.

3.3.1 Bidder Declaration Form (M)

All bidders must complete Exhibit 5, Bidder Declaration GSPD-05-105, and include it with the proposal. When completing the declaration, the bidder must identify all subcontractors proposed for participation in the contract. The bidder awarded the contract is contractually obligated to use the subcontractors for the corresponding work identified, unless the Agency/state entity agrees to a substitution and it is incorporated, in writing. If the bidder is not using subcontractors, complete the form with “Not Applicable” and the bidder’s signature. The form is also available at:

www.documents.dgs.ca.gov/pd/poliproc/MASTER-BidDeclar08-09.pdf

3.4 AMENDMENT

Any contract executed as a result of this solicitation, may be amended, consistent with the terms and conditions of the contract and by mutual consent of both parties, subject to approval by the Statewide Technology Procurement Division under PCC 12100.

3.5 FINANCIAL RESPONSIBILITY INFORMATION

3.5.1 Financial Stability

In order to minimize the potential risk of default due to financial issues, the State reserves the right to request additional documentation throughout the life of the awarded contract.

The State must be assured that the Contractor continues to have the financial resources to sustain their operations during development including the time required for the State to pay the Contractor after project acceptance.

3.5.2 Responsibility Certification (M)

The bidder must certify to the following, to the best of their knowledge and belief that the bidder, the bidder’s subcontractor(s) or any personnel related to the awarded contract:

1. Are not presently debarred, suspended, proposed for debarment, and declared ineligible for the award of contracts by any state or Federal agency.

Bidders must indicate their ability to satisfy this requirements by marking “Yes” on the “Bidder agrees Yes/No” column on Exhibit 4, “Response to Administrative Requirements”. Answering “No” to any of the Mandatory Administrative Requirements in the Final Proposal will result in the proposal being deemed non-responsive, and therefore disqualified.

3.6 CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY

Bidders are advised that deviations from the State approved Terms and Conditions may be grounds for rejection of the proposal.

Bidders are advised that the contract awarded as a result of this solicitation shall automatically include the GSPD – 401IT, *General Provisions – Information Technology revised for CWS-NS Project.*

3.7 COMMERCIAL GENERAL LIABILITY INSURANCE

The Prime Contractor shall maintain general liability with limits of not less than \$1,000,000 per occurrence for bodily injury and property damage liability combined. The policy shall include coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, personal and advertising injury, and liability assumed under an insured agreement. This insurance shall apply separately to each insured against whom a claim is made or suit is brought, subject to the bidder's limit of liability.

In accordance to GSPD – 401IT, General Provisions – Information Technology revised for CWS-NS Project., Section 20, Insurance, the contractor shall furnish insurance certificate(s) evidencing required insurance coverage acceptable to the State, including endorsements showing the State as an “additional insured” if required under the contract. Any required endorsements requested by the State must be separately provided; merely referring to such coverage on the certificates(s) is insufficient for this purpose. When performing work on state owned or controlled property, contractor shall provide a waiver of subrogation in favor of the State for its workers’ compensation policy.

The Prime Contractor shall agree to furnish the State satisfactory evidence thereof within ten (10) calendar days of contract award.

3.8 ADMINISTRATIVE REQUIREMENTS DOCUMENT (M)

Bidders must indicate their willingness and ability to satisfy these requirements by marking “Yes” on the “Bidder agrees Yes/No” column on Exhibit 4, “Response to Administrative Requirements”. Answering “No” to any of the Mandatory Administrative Requirements in the Final Proposal will result in the proposal being deemed non-responsive, and therefore disqualified.

3.9 COVER LETTER (M)

The Bidder must submit a cover letter containing the following:

1. Be on company letterhead;

2. Include the legal name of the Bidding organization;
3. Include the address of the Bidder's organization;
4. Include a statement that the proposal response is the Bidder's binding offer, good for 180 calendar days from scheduled Contract Award date, as noted in subsection 2.3, KEY ACTION DATES;
5. Include a statement indicating that the bidder agrees to the terms and conditions of this solicitation and accepting responsibility as the Prime Contractor if awarded the contract resulting from this solicitation;
6. Include a statement indicating that the bidder has available staff with the appropriate skills to complete the contract for all services and provide all deliverables as described in this solicitation;
7. Be signed by an individual who is authorized to bind the bidding firm contractually. The individual's name must also be typed, and include the title or position that the individual holds in the firm. An unsigned Final Proposal may be rejected;
8. Include the email and phone number of the person signing the letter;
9. Include the date signed.

3.10 STD. 213, STANDARD AGREEMENT (M)

The STD. 213, Standard Agreement must be signed by a party authorized to bind the firm contractually. Bidders shall complete and submit Exhibit 1, STD. 213 Standard Agreement and attach it to the Statement of Work.

The Bidder shall only complete the "CONTRACTOR'S NAME" in block 1, and all of the information required for the "CONTRACTOR" block in the lower part of Exhibit 1, STD. 213. **DO NOT INCLUDE ANY DOLLAR FIGURES.**

Bidders are advised that deviations to the STD. 213 may be grounds for rejection of their proposal.

3.11 STATEMENT OF WORK (M)

The Statement of Work (SOW) identifies and describes the tasks and responsibilities of the contractor and the responsibilities of the State during the contract. The Bidder shall submit the SOW with the Exhibit 1, STD. 213 as part of the final proposal response. Bidders are advised that deviations to the SOW may be grounds for rejection of their proposal.

3.12 CONFIDENTIALITY STATEMENT (M)

Bidders must agree to the State's confidentiality requirements by submitting a signed Exhibit 3, Confidentiality Statement, for the bidder's firm. The completed Confidentiality Statement must be submitted with the Intent to Bid, Exhibit 2 as indicated in subsection 2.3, KEY ACTION DATES.². The bidder will also be required, upon contract award, to submit a signed Confidentiality Statement from all employees and subcontractor staff assigned to the awarded contract.

The bidder engaging in services pertaining to this solicitation, requiring contact with confidential State information or State customer information will be required to exercise security precautions for all such data that is made available and must accept full legal responsibility for the protection of this confidential information. This includes all statistical, personal, technical and/or other confidential personal data and information relating to the State's operations that are designated confidential by the State.

3.13 SECRETARY OF STATE CERTIFICATION (M)

If required by law, the Prime Contractor must submit a Certificate of Status from California Secretary of State, showing that the Prime Contractor is certified with the California Secretary of State to do business in the State of California. If the bidder does not currently have this certification, the firm must be certified before a contract award can be made, and must provide information in the Final Proposal to support the status of its application to be certified to do business in the State of California.

Domestic and foreign Corporations, Limited Liability Companies (LLCs), Limited Liability Partnerships (LLPs) and Limited Partnerships (LPs) must be registered with the California Secretary of State to be awarded the contract. The California Secretary of State Certificate of Status must be included with the proposal. The required document(s) may be obtained through the California Secretary of State, Certification and Records Unit at (916) 657-5448 or through the following website: <http://kepler.sos.ca.gov/>, refer to Exhibit 6.

3.14 WORKERS COMPENSATION (M)

The Prime Contractor must maintain statutory Workers' Compensation for all its employees who will be engaged in the performance of the contract, and agree to furnish the State satisfactory evidence thereof at the time the State may so request. The bidder is required to sign Exhibit 7, Workers' Compensation Certification, and submit it with the proposal response.

² Exhibit 3, Confidentiality Statement, must be included in the Final Bid and/or prior to bidder's access to Bidders' Library.

3.15 SELLER'S PERMIT (M)

This proposal is subject to all requirements set forth in §6452, §6487, §7101 and §18510 of the Revenue and Taxation Code §10295 of the Public Contract Code, requiring bidders to provide a copy of their retailer's seller's permit or certification of registration and, if applicable, the permit or certification of all participating affiliates issued by the State of California's Board of Equalization. For more information on seller's permit or certification of registration, refer to the following link: <http://boe.ca.gov/pdf/pub73.pdf>, refer to Exhibit 8.

3.16 PAYEE DATA RECORD (STD. 204) (M)

The Payee Data Record (STD.204) indicates the bidder is subject to state income tax withholdings pursuant to California Revenue and Taxation Code §18662.

Bidders must complete Exhibit 9, Payee Data Record, and submit it with their proposal. The bidder must provide the company's Federal Employer Identification Number (Business IRS Number) with their final proposal submission on this form. The form can be located at the following website: <http://www.documents.dgs.ca.gov/dgs/fmc/pdf/std204.pdf>

3.17 IRAN CONTRACTING ACT OF 2010 (M)

Division 2, Part 1, Chapter 2.7 of the PCC is the Iran Contracting Act of 2010. This Act §2203 requires that no one shall submit a proposal for a contract, or enter into or renew a contract, with a public entity for goods or services valued at \$1,000,000 or more if that person (i.e., bidder or contractor) engages in investment activities of \$20,000,000 or more as described in PCC §2202.5 pursuant to all provisions of the Iran Contracting Act of 2010. The Iran Contracting Act of 2010, at §2204 requires bidders to certify at the time the proposal is submitted or the contract is renewed, that the person is not identified on a list created pursuant to subdivision (b) of PCC §2203 as a person engaging in investment activities in Iran described in subdivision (a) of PCC §2202.5, or as a person described in subdivision (b) of PCC §2202.5, as applicable.

Bidders must complete Exhibit 10, Iran Contracting Act of 2010, and submit with their Final Proposal, and again each time their awarded contract is renewed.

3.18 BIDDING PREFERENCE PROGRAMS**3.18.1 Disabled Veteran Business Enterprise (DVBE) Program (O)**

The Disabled Veteran Business Enterprise (DVBE) Participation Goal Program for State contracts are established in Public Contract Code (PCC), §10115 et seq., Military and Veterans Code (MVC), §999 et seq., and California Code of Regulations (CCR), Title 2, §1896.60 et seq.

PLEASE READ THESE REQUIREMENTS CAREFULLY. FAILURE TO COMPLY WITH THE MINIMUM DVBE PARTICIPATION REQUIREMENT WILL CAUSE YOUR SOLICITATION RESPONSE TO BE DEEMED NONRESPONSIVE AND YOUR FIRM INELIGIBLE FOR AWARD OF THE PROPOSED CONTRACT.

3.18.1.1 DVBE Participation Requirement (M)

Bidders must fully comply with DVBE Participation Program requirements in the Draft Proposal and Final Proposal. Failure to submit a complete response will result in a non-responsive determination, in which case the Final Proposal will be rejected. The minimum DVBE participation goal is three percent (3%) for this solicitation. The DVBE Program requirements information may be viewed at:

http://www.documents.dgs.ca.gov/pd/poliproc/Master-DVBEIncentiveRequireGoodIT11_1215.pdf.

The bidder must complete and submit Exhibit 5, GSPD-05-105 Bidder Declaration with their Final Proposal. This form and its completion instructions may be accessed at:

<http://www.documents.dgs.ca.gov/pd/poliproc/master-biddeclar08-09.pdf>

The bidder who has been certified by California as a DVBE (or who has obtained the participation of subcontractors certified by California as a DVBE) must also submit a completed form(s) STD.843 Disabled Veteran Business Declarations. All disabled veteran owners and disabled veteran managers of the DVBE(s) must sign the form(s). Exhibit 12, STD.843 Disabled Veteran Business Declarations form may be accessed at:

www.documents.dgs.ca.gov/pd/poliproc/STD-843FillPrintFields.pdf

The Office of Small Business and DVBE Services offer program information and may be reached at:

Office of Small Business and DVBE Services
707 Third Street, 1st Floor, Room 400
West Sacramento, CA 95606

<http://www.dgs.ca.gov/pd/Programs/OSDS.aspx>

Receptionist: (916) 375-4940 Fax (916) 375-4650

3.18.1.2 DVBE Participation Incentive (M)

In accordance with §999.5(a) of the Military and Veterans Code, an incentive will be given to bidders who exceed the three percent (3%) DVBE mandatory participation. For Contract Award evaluation purposes only, the State shall apply the incentive amount based on the amount of DVBE participation obtained above the three percent (3%) requirement. The incentive is only

given to those bidders who are responsive to the DVBE Program Requirement and propose DVBE participation in the resulting contract that exceeds the mandatory three percent (3%) requirement. If bidder is claiming a DVBE preference, the bidder must complete and submit Exhibit 5, GSPD-05-105 Bidder Declaration and Exhibit 13, Bidding Preferences and Incentives. If bidder is not using subcontractors, complete and sign Exhibit 5 with "Not Applicable". See Section 7, EVALUATION, for details on the amount and application of the incentive during proposal evaluation.

3.18.2 Small Business Preference (O)

§14835 et seq. of the California Government Code requires that a five percent (5%) preference be given to bidders who qualify as a small business. The rules and regulations of this law, including the definition of a small business, or qualifying non-small business, are contained in Title 2, California Code of Regulations, §1896 et seq. The definition of nonprofit veteran service agencies qualifying as a small business is contained in §999.50 et seq. of the Military and Veterans Code. Bidders must complete and submit Exhibit 13, Bidding Preferences and Incentives and Exhibit 5, GSPD-05-105 Bidder Declaration. If bidder is not using subcontractors, complete and sign Exhibit 5 with "Not Applicable". More information regarding the Small Business Preference may be found at: www.dgs.ca.gov/pd/Programs/OSDS.aspx

3.18.3 Non-Small Business Preference (O)

A five percent (5%) proposal preference is available to bidders who qualify as a non-small business claiming at least 25 percent (25%) California-certified small business subcontractor participation. If claiming the non-small business subcontractor preference, the bidder's response must include a list of the small business(es) with which the firm commits to subcontract in an amount of at least 25 percent (25%) of the net proposal price with one (1) or more California-certified small businesses. Each listed certified small business must perform a "commercially useful function" in the performance of the contract as defined in Government Code §14838(b)(1)(2).

Bidders claiming the five percent (5%) preference must commit to subcontract at least 25 percent (25%) of the net proposal price with one (1) or more California-certified small businesses. Completed certification applications and required support documents must be submitted to the Office of Small Business and DVBE Services (OSDS) no later than 5 p.m. of the proposal due date, and the OSDS must be able to approve the application as submitted. Questions regarding certification should be directed to the OSDS at (916) 375-4940.

The preference to a non-small business firm that commits to small business or microbusiness subcontractor participation of 25 percent (25%) of its net proposal price shall be five percent (5%) of either the lowest responsive, responsible firm's price or the highest responsive,

responsible firm's total score. A non-small business, which qualifies for this preference, may not take an award away from a certified small business.

If claiming a Small Business preference or using Small Business subcontractors, the bidder must complete and submit Exhibit 5, GSPD-05-105 Bidder Declaration and Exhibit 13, Bidding Preferences and Incentives. If bidder is not using subcontractors, complete and sign Exhibit 5 with "Not Applicable".

3.18.4 Commercially Useful Function (M)

If the bidder is a California-Certified SB, in accordance with AB 669 (Chapter 623, Statutes of 2003), the bidder must address specific aspects of the legislation that requires Certified Small Businesses to perform a Commercially Useful Function as defined by Government Code §14837, §14838.6, §14839, §14842, and §14842.5.

A contractor, subcontractor, or supplier will not be considered to perform a Commercially Useful Function if the contractor's subcontractor's, or supplier's role is limited to that of an extra participant in the transaction, the awarded contract, or project through which funds are passed to obtain the appearance of small business or micro business participation.

Bidders must complete Exhibit 14, Commercially Useful Function (CUF) Certification. All bidders and subcontractors identified in the proposal response to fulfill the requirements for one (1) or more of the socio-economic programs (DVBE and small business) must perform a commercially useful function (CUF) in the resulting contract. CUF is defined pursuant to Military and Veterans Code §999(b)(5)(B) and Government Code §14837(d)(4)(A) for the DVBE and small business programs, respectively.

Bidders claiming one (1) or more of the socio-economic programs must complete and submit as part of the Final Proposal response, Exhibit 5, GSPD-05-105 Bidder Declaration, also available at: www.documents.dgs.ca.gov/pd/poliproc/MASTER-BidDeclar08-09.pdf. If bidder is not using subcontractors, complete and sign Exhibit 5 with "Not Applicable".

Bidder(s) may be required to submit additional written clarifying information regarding CUF on Exhibit 14, Commercially Useful Function Certification. Failure to submit the requested written information as specified may be grounds for proposal rejection.

3.18.5 Target Area Contract Preference Act (TACPA) (O)

Target Area Contract Preference will be granted to California-based firms in accordance with Government Code §4530 whenever contracts for goods or services are in excess of \$100,000 and the bidder meets certain requirements as defined in the California Administrative Code (Title 2, §1896.30 et seq.) regarding labor needed to produce the goods or provide the services being procured. The Target Area Preference is optional on the part of the bidder (not

mandatory), is for proposal evaluation purposes only, and does not alter the amount of the awarded contract. Bidders desiring to claim Target Area Contract Preference Act (TACPA) preference shall complete and submit Exhibit 15, STD 830 Target Area Contract Preference Act – Preference Request for Goods and Services and Exhibit 13, Bidding Preferences and Incentives. The STD 830 is also available at: <http://www.documents.dgs.ca.gov/dgs/fmc/pdf/std830.pdf>. Additional instructions are provided on the form.

3.19 PRODUCTIVE USE REQUIREMENTS (M)

The Productive Use Requirements protects the State from being an experimentalist for new equipment and software having no record of proven consistent performance. The State will only accept proven technology products.

To the extent that the proposed solution includes equipment and off-the-shelf software, it must be currently supported by its manufacturer for at least the time specified in Table 3-2, Productive Use Timeframes. No equipment and/or software may be proposed, specified, or employed if the manufacturer has announced an end to support. The productive use requirements defined in this subsection do not apply to any portion of the custom software developed or modified for the State under this contract prior to proposed submittal and throughout contract duration.

3.19.1 Customer In-Use (M) (If Applicable)

The State requires each equipment and software component proposed as part of an automated system adhere to the following:

1. Must have been installed and in productive use, in substantially the conformation bid;
2. For a paying customer external to the bidder's organization; and
3. For at least the number of months shown in the table below and prior to the required date of installation or Final Proposal submission.

Table 3-2: Productive Use Timeframes

Product	Project Cost	Installation	Final Proposal Submission
Category 1 - Critical Software Software that is required to control the overall operation of a computer system or peripheral equipment. Included in this category are operating systems, data base management systems, language interpreters, assemblers and compilers, communications software, and other essential system software.	{Less than \$10,000}	1 month	1 month
	{\$10,000 up to \$100,000}	4 months	3 months
	{More than \$100,000}	8 months	6 months
Category 2 - All Information Technology Equipment and Non-critical Software. Information technology equipment is defined in SAM §4819.2.	{Less than \$10,000}	1 month	1 month
	{\$10,000 up to \$100,000}	4 months	3 months
	{More than \$100,000}	6 months	4 months

Design changes in required system control modules or in components critical to the processing requirements of the State's workload are also subject to the In-use requirement. Increases or decreases in numbers of components or minor alteration in equipment or minor modifications or updates to software to provide improvements or features, to correct errors, or to accommodate hardware changes may be exempt from the In-use requirement by the Department of Technology, Statewide Technology Procurement Division, if no changes in logic, architecture or design are involved.

3.19.2 Customer References for Productive Use Requirements (M) (If Applicable)

The purpose of the Customer Reference requirement is to provide the State the ability to verify the claims made in the proposal by the bidder.

The bidder must provide a list of customers who presently have the bid equipment and/or software installed and operating. If subsection 3.20.1, Customer In-Use, is used, the list must include at least one (1) customer meeting that requirement. However, at least one customer reference must be included for each type of machine and feature bid that is subject to the requirements of that subsection (i.e., one customer having the specific CPU).

The State has the option to request from the bidder supporting evidence of compliance to the Customer In-Use requirements. Supporting evidence could include, but is not necessarily limited to, one or more of the following:

- Customer Purchase Order or contract showing installation dates for subject equipment or software;
- Acceptance Document containing verification of installation by a paying customer;
- Customer Invoice for subject equipment or software;
- Shipping Invoice or Bill of Lading;
- Dated Maintenance Records;
- Sworn Notarized Statement from an officer of the bidding firm and/or a paying customer;
- State visit to the site of a paying customer.

The State will not consider exceptions to Productive Use Requirements for this solicitation.

3.19.3 Equipment (M) (If Applicable)

All equipment offered must be new and the latest model in current production. Used, shopworn, refurbished, demonstrator, prototype, or discontinued models are not acceptable.

3.20 LAWS TO BE OBSERVED

3.20.1 Labor

Pursuant to §1775 of the California Labor Code, the contractor shall, as a penalty to the State or political subdivision on whose behalf the contract is made or awarded, forfeit not more than fifty dollars (\$50) for each calendar day, or portion thereof, for each worker paid by the contractor, or its subcontractor, less than the prevailing wage so stipulated; and in addition, the contractor further agrees to pay to each worker the difference between the actual amount paid for each calendar day, or portion thereof, and the stipulated prevailing wage rate for the same. This provision shall not apply to properly registered apprentices.

Pursuant to §1810-§1815 of the California Labor Code, inclusive, it is further agreed that the maximum hours a worker is to be employed is limited to eight (8) hours a day and forty (40) hours a week and the contractor shall forfeit, as a penalty to the State, twenty-five dollars (\$25) for each worker employed in the execution of the contract for each calendar day during which a worker is required or permitted to labor more than eight (8) hours in any calendar day or more than forty (40) hours in any calendar week, in violation of §1810-§1815 of the California Labor Code, inclusive.

3.20.2 Travel and Subsistence Payments

The contractor shall pay the travel and subsistence of each worker needed to execute the work, as such travel and subsistence payments are defined in the applicable collective bargaining agreements filed in accordance with California Labor Code §1773.8.

3.20.3 Apprentices

Special attention is directed to §1777.5, §1777.6, and §1777.7 of the California Labor Code and Title 8, California Code of Regulations §200 et seq. Each contractor and/or subcontractor must, prior to commencement of the public works contract, contact the Division of Apprenticeship Standards, 525 Golden Gate Avenue, San Francisco, CA, or one of its branch offices to insure compliance and complete understanding of the law regarding apprentices and specifically the required rationale thereunder. Responsibility for compliance with this section lies with the Prime Contractor.

3.20.4 Payroll

The contractor shall keep an accurate payroll record showing the name, address, Social Security Account Number, work classification and straight time and overtime hours worked by each employee. A certified copy of the employee's payroll record shall be made available for inspection as specified in §1776 of the California Labor Code.

4. BID REQUIREMENTS

This Section 4 contains the Mandatory Bid Requirements that must be met in order to be considered responsive and responsible to this solicitation. Unless designated otherwise, all of the requirements in this section are mandatory; however, the documents that must be submitted with the bidder's Final proposal are noted as Mandatory "(M)" or Mandatory Scored "(MS)".

1. (M) Items labeled "Mandatory" or "M" are not negotiable. To be considered responsive and responsible to these requirements, all requirements identified as (M) must be responded to. A "Fail" will result in a proposal being deemed non-responsive and, therefore, will be disqualified. Failure to respond to any (M) requirements where indicated shall result in disqualification of the proposal.
2. (MS) Items labeled "Mandatory Scorable" or "MS" are not negotiable. To be considered responsive and responsible to these requirements, all requirements identified as (MS) must be responded to. A "Fail" will result in a proposal being deemed non-responsive and, therefore, will be disqualified. Failure to respond to any (MS) requirements where indicated shall result in disqualification of the proposal. The State's evaluation team will review responses to (MS) requirements and apply points, if applicable, per criteria stated in Section 7, EVALUATION.

4.1 Qualification Requirements

The bidder is expected to have a proven record of success and be responsible for all aspects of the service, including any subcontractors and the project team/staff proposed.

Bidders must meet the minimum Bidder Qualification and Staff Qualification Requirements. Failure to meet any of the minimum requirements shall result in a proposal being deemed non-responsive and therefore disqualified.

4.1.1 Bidder Qualifications (M)

Bidders must complete and submit as part of the proposal response, Exhibit 18.1, Bidder Qualification Form, to confirm that the bidder's experience meets all the minimum requirements indicated. It is incumbent on the bidder to provide enough detail in the response for the State to evaluate the bidder's ability to meet the requirements and perform the services as described in this solicitation. Bidders must provide information for a minimum of three (3) projects. A separate Exhibit 18.1, Bidder Qualification Form must be submitted for every project used to meet the minimum required experience. One (1) project may meet multiple

requirements, but at least three (3) projects and not more than six (6) projects must be provided to meet the requirements in Exhibit 18.1, Bidder Qualification Form.

4.1.2 Bidder References (M)

Bidders must complete and submit as part of the proposal response, Exhibit 18.2, Bidder Reference Form, for each of the projects cited on the corresponding Exhibit 18.1, Bidder Qualification Form.

References may be contacted to validate submitted responses based on customer satisfaction in accordance with Section 7, EVALUATION. References must be external to a bidder's organization and corporate structure.

Failure to provide verifiable references may cause the proposal to be rejected. The purpose of the bidder References requirement is to provide the State the ability to assess the bidders' prior record and experience in providing similar or relevant services to other organizations. The description of their projects must be detailed and comprehensive enough to permit the State to assess the similarity of those projects to the work anticipated for the contract resulting from this procurement. References must include all information required on Exhibit 18.2, Bidder Reference Form.

Exhibit 18.2, Bidder Reference Form, must be completed in its entirety, signed, and dated by a client reference contact that performed a management or supervisory role on the reference project to be considered responsive. The Exhibit 18.2, Bidder Reference Forms must be returned to the bidder for submission with the proposal. Photocopies will be accepted as long as the form, response, and signature are legible. No information corrections or changes may be made on the reference form by the bidder. Forms with alterations or changes to the entered information may be rejected.

If the client reference is not allowed either legally or by company/organization policy to sign the client reference form, the client reference must type in their full name with a brief statement on the form outlining the reason they are not permitted to sign the States reference form. If needed, the State may contact either the bidder and/or Staff References to validate the reference submitted. The Evaluation Team will make two (2) attempts via email to validate bidder and/or staff experience using the information provided in the bidder and/or Staff Reference forms, as applicable.

4.1.3 Staff Qualifications (M)

Bidder is fully responsible for all necessary staffing resources to successfully meet all requirements in its contract within the agreed upon schedule and to perform to the standards set forth in the SOW.

Bidders must complete and submit as part of the proposal response Exhibits 19.1 through 19.8, Staff Qualifications Forms, the bidder must provide complete information to confirm each of the proposed staff possess the experience and qualifications as specified for their project role described in Exhibits 19.1 through 19.8, Staff Qualifications Forms. Bidders per proposed staff to meet the requirements. Each cited project for each staff proposed must be submitted separately on Exhibits 19.1 through 19.8, Staff Qualifications Forms. References may be contacted to verify staff's experience qualification information. References must be external to a bidder's organization and corporate structure.

4.1.4 Staff References (M)

The purpose of the Staff References requirement is to provide the State the ability to assess the staff's experience in providing similar or relevant services to other organizations. The description of their projects must be detailed and comprehensive enough to permit the State to assess the similarity of those projects to the work anticipated for the contract resulting from this procurement.

Bidders must provide at least three (3) projects and not more than six (6) projects as part of the proposal response, Exhibits 19.2 through 19.8, Staff Reference Forms, to confirm that the staff experience meets the minimum requirements indicated. The bidder must submit a completed Staff Reference Form for each project cited in Exhibits 19.2 through 19.8. References must complete all required information on the Staff Reference Forms. It is incumbent on the bidder to provide enough detail in the response for the State to evaluate the bidder's proposed staff's ability to meet the requirements and perform the services as described in this solicitation.

References may be contacted to validate submitted responses and points will be awarded based on experience in accordance with Section 7, EVALUATION. (References must be external to a bidder's organization and corporate structure.). Failure to provide verifiable references may cause the proposal to be rejected.

Exhibits must be completed in their entirety, signed, and dated by a client reference contact that performed a technical or supervisory role on the referenced project to be considered responsive. Photocopies will be accepted as long as the form, response, and signature are legible. No information corrections or changes may be made on the staff reference forms. Forms with alterations or changes to the entered information may be rejected.

If the Client reference is not allowed either legally or by company/organization policy to sign the Client reference form, the Client reference must type in their full name with a brief statement on the form outlining the reason they are not permitted to sign the States reference form. If needed, the State may contact either the bidder and/or Staff References to validate the reference submitted. The Evaluation Team will make two (2) attempts via email to validate bidder and/or Staff experience using the information provided in the bidder and/or Staff Reference forms, as applicable.

4.1.4.1 Full-Time/Part-Time Month Equivalents Definition

For each experience requirement (marked by “x”) that is met by the staff person’s work on the referenced project, specify the number of full-time month equivalent experience that the staff person accrued on the referenced project. For each period in which the staff person performed work applicable to the claimed experience for a minimum of twenty (20) work days of a minimum total of 140 hours (the minimum required to represent working full-time), the staff accrues one (1) full-time month equivalent experience. To calculate and report the full-time month equivalent experience for staff who worked part-time (partial) on a referenced project, use the following calculation:

If the staff worked half ($\frac{1}{2}$) time on a referenced project, experience should be pro-rated to one-half ($\frac{1}{2}$) or 0.5 month full-time month equivalent experience for each period in which the staff person worked a minimum of seventy (70) hours over twenty (20) work days in a month.

For each experience requirement that the staff’s work on a referenced project addresses, report the total number of full-time month equivalents’ experience the staff’s work represents using the calculations as previously described in this section, which depend upon the time period during which the staff worked on the referenced project and whether he/she worked on a full-time or some other basis.

4.2 SOLUTION REQUIREMENTS

4.2.1 Contractor Requirements (Functional and Non Functional Requirements) (M)

Bidders must complete the following exhibits and include each exhibit in their Final Proposal in accordance with Section 4, BID REQUIREMENTS and Section 6, PROPOSAL/BID FORMAT AND SUBMISSION REQUIREMENTS:

1. Exhibit 20 – Functional and Non Functional Requirements (M)

The Bidder must indicate compliance and confirmation with each of the requirements located in the SOW. The Bidder must complete and submit as part of the bid response, Exhibit 20, Functional and Non Functional Requirements certifications.

2. Exhibit 21. – Proposal Narrative Requirements (MS)

Bidders shall complete Exhibit 21 Proposal Narrative Requirements and provide a narrative response for each bidder proposal requirement description.

Bidders are reminded that in order to be considered responsive and responsible to the requirement, the bidders must provide enough detail in their response in order for the State to evaluate the bidder's ability to meet the requirement. Refer to Section 7, EVALUATION for details on how the requirement will be scored as part of the overall evaluation.

5. COST

Cost is a primary evaluation criterion weighted at thirty percent (30%) of the total points. Evaluation in this category will be based on the lowest total estimated net cost as calculated according to the methodology in this section and Section 7, EVALUATION.

The intent is to structure the pricing format in order to facilitate a straightforward comparison among all bidders and foster competition to obtain the best market pricing. Each bidders' cost must be in the format outlined in this section. Bidders are advised that failure to comply with the instructions listed in this section, such as submission of incomplete proposals or use of alternative pricing structures or different formats than the one requested, may result in the rejection of their proposals...

Important Note: It is imperative that no cost information be included in the body of the proposal. Cost information shall only be submitted in a separately sealed container in the bidder's Response, Volume 3, Cost Data in accordance with Section 6, PROPOSAL/BID FORMAT AND SUBMISSION REQUIREMENTS.

5.1 Payment Method

Payment to the Contractor will be made on a time and materials basis per the hourly labor classifications set forth in the Cost Worksheet. The payment amount for each Sprint is capped at a total of each resource's labor classification rate multiplied by 90 hours. A Sprint is defined as a two (2) week period.

5.2 Payment Frequency

Payment shall be made after the completion and acceptance for two Sprints (i.e. every four weeks).

5.3 Payment Withhold

To ensure satisfactory performance by the Contractor and mitigate risk to the State, the State will withhold ten percent (10%) from each payment. The State will release the Withhold

payment to the Contractor at the conclusion of the entire Contract, provided that all accepted user stories have achieved the Release-level Definition of Done.

5.4 Cost Workbook Instructions

In order to capture all proposed costs, the State has developed a pre-formatted Microsoft Excel® Cost Workbook for the Bidder to enter and submit cost data with its Final Proposal. This subsection includes instructions for completing Exhibit 22, Cost Workbook.

The Bidder is responsible for entering cost information in the format prescribed in Exhibit 22, Cost Workbook. Cells that are shaded grey are protected cells used to indicate headings, automatically calculate summary numbers, or are other areas in which the Bidder does not need to enter or alter information. Cells that are shaded green are those cells the Bidder is expected to complete.

The Bidder may insert additional rows in select worksheets, as needed, using an integrated “Insert Row(s)” macro provided at the bottom of each relevant worksheet. The integrated macro ensures that new rows inserted maintain appropriate formatting and formulas. To use, highlight the last row in the data set, click on the macro, enter the number of rows that needs to be inserted, and then press “ok.” The Bidder must ensure that all worksheet links and calculations are correct.

Exhibit 22, Cost Workbook, includes the cost worksheets listed in Table 5.1, Cost Worksheets, each of which is described in the subsections that follow:

Table 5.1 Cost Worksheets

Sheet #	Worksheet Name	
1.	Main Menu	
2.	Worksheet 5-1	Cost Evaluation
3.	Worksheet 5-2	Contract Cost
4.	Worksheet 5-3	Labor Rates
5.	Worksheet 5-4	Labor Costs
6.	Worksheet 5-5	Software Costs

Main Menu

This worksheet captures the Bidder's name and the State's assumptions for calculating labor costs. The only information the Bidder needs to enter on this worksheet is their name.

Worksheet 5-1 Cost Evaluation

This worksheet summarizes the costs from all other worksheets and calculates the Bidder's Cost Proposal used for evaluation. The Bidder must not modify or enter any fields on this worksheet.

Worksheet 5-2 Contract Cost

This worksheet calculates the proposed base period and optional period amounts to arrive at the total contract cost. This worksheet is automatically populated using cost information extracted from other worksheets. The Bidder must not modify or enter any fields on this worksheet.

Worksheet 5-3 Labor Rates

This worksheet captures the labor classifications, descriptions of labor classifications and hourly rates used throughout the term of the contract. Table 5.2, Labor Rates Worksheet Instructions, guides the Bidder to make all appropriate entries in Worksheet 5-3.

Table 5.2 Labor Rates Worksheet Instructions

Column	Column Heading	Instructions
Column B	Labor Classification	Enter all proposed labor classifications on separate lines required to complete the work as described in the Statement of Work (SOW).
Column C	Description	Enter a description for each labor classification. The description should be robust enough to ensure the State has a general understanding of the work to be performed for each labor classification.
Column D	Hourly Rate	Enter the hourly rate for each labor classification.

Worksheet 5-4 Labor Costs

This worksheet captures the labor costs of the base period and each optional period that will be used as a basis of payment throughout the term of the contract. Table 5.3, Labor Costs Worksheet Instructions, guides the Bidder to make all appropriate entries in Worksheet 5-4.

Table 5.3 Labor Costs Worksheet Instructions

Column Heading	Instructions
Labor Classification	No entry required. The labor classifications entered in Worksheet 5-3 will be copied to this column.
# of Hours	No entry required. The information used to calculate the number of hours is provided in the Main Menu Worksheet under the Assumptions heading for the base period and each optional period. It multiples the number of weeks by the number of hours per week for the base period and each optional period.
Hourly Rate	No entry required. The hourly rates entered in Worksheet 5-3 will be copied to this column.
Total	No entry required. This multiplies the # of hours column by the hourly rate column to arrive at the total cost per labor classification for base period and each optional period.

Note: If the Bidder enters additional lines in Worksheet 5-3, the Bidder must enter the same number of lines at the bottom of this Worksheet.

Worksheet 5-5 Software Costs

This worksheet is used to identify all software and its associated costs. Table 5.4 Software Costs Worksheets Instructions, guides the Bidder to make all appropriate entries in Worksheet 5-5.

Table 5.4 Software Costs Worksheets Instructions

Column	Column Heading	Instructions
Column B	Software Name/Product Number/Version	Enter a brief description identifying the software product, which includes the name, product number, and version. Different software products must be identified in separate lines.
Column C	License Type	Enter the type of software license. The State requires that all software products be an enterprise license unless the Bidder can demonstrate that an alternative licensing approach will be more cost effective for the State.
Column D	Quantity	Enter the quantity for each software product for the proposed solution.
Column E	Unit Cost	Enter the unit cost for each software product, inclusive of all taxes, fees, freight, and other charges, if applicable.

Column	Column Heading	Instructions
Column F	Total Unit Maintenance Cost	Enter the total unit maintenance cost for each software product, if applicable.
Column G	Extended Cost	No entry required. This column will automatically populate using a formula that will multiply the quantity in Column D by the unit cost identified in Column E.
Column H	Extended Maintenance	No entry required. This column will automatically populate using a formula that will multiply the quantity in Column D by the unit maintenance cost identified in Column F.
Column I	Total Cost	No entry required. This column will automatically populate the total cost of the hardware using a formula that adds Column G and Column H.

6. PROPOSAL/BID FORMAT AND SUBMISSION REQUIREMENTS

These instructions identify the mandatory proposal format and the approach for the development and presentation of proposals. Format instructions must be followed, all requirements and questions in the solicitation must be answered and all requested data must be supplied. The bidder shall carefully examine the solicitation and be satisfied with the compliance conditions prior to submitting a proposal.

It is important that all proposals be submitted in sealed envelopes/containers and clearly marked or they may be rejected. Proposal submittals must be in the number of copies indicated in Section 6, PROPOSAL/BID FORMAT AND SUBMISSION REQUIREMENTS.

The State will not be liable for any costs incurred by any bidder in responding to this solicitation, regardless of whether the State awards the contract through this process, decides not to move forward with the project, cancels this solicitation for any reason, or contracts for the Project through other processes or by issuing another solicitation.

6.1 Preparation

Proposals are to be prepared in such a way as to provide a straightforward, concise delineation of capabilities to satisfy the requirements of this solicitation document. Expensive bindings, colored displays, promotional materials, etc., are not necessary or desired. Emphasis should be concentrated on conformance to the solicitation document instructions, responsiveness to the solicitation document requirements, and completeness and clarity of content.

6.2 Completion of Proposals

Proposals must be complete in all respects as required by Section 6, PROPOSAL/BID FORMAT AND SUBMISSION REQUIREMENTS. A Final Proposal may be rejected if it is conditional or incomplete, or if it contains any alterations of form or other irregularities of any kind. A Final Proposal must be rejected if any such defect or irregularity constitutes a material deviation from the solicitation document requirements. The Final Proposal must contain all costs as required in Section 5, COST and Section 6, PROPOSAL/BID FORMAT AND SUBMISSION REQUIREMENTS.

6.3 Date, Time, and Address of Submittals

Mail or deliver proposals to the Procurement Official listed in subsection 2.2.1. If mailed, it is suggested that bidders use certified or registered mail with return receipt requested, as delivery of documents is at the bidder's own risk of untimely delivery, lost mail, etc.

Proposals must be received no later than the date and time specified in subsection 2.3, KEY ACTION DATES. A proposal not received by the date and time specified in subsection 2.3, KEY ACTION DATES, shall be rejected.

6.4 Packaging and Labeling

Bidders may provide all of their proposal documents at the same time within the same package (box or boxes). The overall package shall be sealed and labeled as follows:

1. The bidder's name and address
2. The solicitation number " RFP OSI 31326"
3. Identification of the submittal as "RFP OSI 31326" Final Proposal
4. Box "# of #", if more than one (1) box is required for the entire submission

Each Binder and Cd Must Be Plainly Marked With:

1. The bidder's name
2. The solicitation number "RFP OSI 31326"
3. Identification of the submittal as "RFP OSI 31326" Part 1 or Part 2
4. The Volume number and title as appropriate:
 - a. Volume 1 – Response to Section 3, ADMINISTRATIVE REQUIREMENTS, and Section 4, BID REQUIREMENTS
 - b. Volume 2 – Std. 213 and Statement of Work
 - c. Volume 3 – Cost

Volume 3, Cost Information, (both binder and CDs) should be in its own sealed package (or envelope) that is separate from Volumes 1, 2, 4. If the Cost Information is not submitted in its own separately sealed package (or envelope), the proposal may be rejected.

6.5 Formatting

It is the bidder's responsibility to ensure its proposal is submitted in a manner that enables the State to easily locate all response descriptions and exhibits for each requirement of this solicitation. Page numbers should be located in the same page position throughout the proposal. Each page should be numbered with the section reference (e.g. Section 3, page 3 of 21) to make easy reference possible. Figures, tables, charts, etc., should be assigned index numbers and should be referenced by these numbers in the text and in the table of contents. Figures, tables, charts, etc., should be placed as close to text references as possible. The proposal should be tabbed, to identify the volume and section.

Proposals must be submitted in printed format (hard copy), and also in electronic file format (soft copy) on a CD:

1. All hard copies must be on standard 8.5" x 11" paper, except for charts, diagrams, and similar materials, which may be foldouts. If foldouts are used, the folded size must fit within the 8.5" x 11" format. Hard copy of large size drawings shall not be larger than Standard E-size format.
2. Double sided printing is preferred. The following must be shown on each page of the Proposal:
 - a. RFP OSI 31326
 - b. Name of bidder
 - c. Volume number
 - d. Part and/or Exhibit Number
 - e. Page number (Page # of ##)
3. Soft copies of the proposals must be in Microsoft Word 2010 and Excel 2010 as appropriate, or compatible, except electronic files of drawings shall be compatible with Microsoft Visio 2010.
4. Each Volume submitted shall be provided in the following number of copies:
 - a. Five (5) hard copies (printed), one (1) copy marked Master, for a total of six (6) copies.
 - b. Two (2) soft copies (CD's or a USB compatible portable data storage device)
5. All hard copy submittals should use clearly marked tabs, page numbers and table of contents for effective access to the bidder's material. Similarly, soft copies should be organized into appropriate files and folders designed for easy access. The MASTER COPY

must contain original signatures or initials wherever a signature or initials are required. If discrepancies exist between two (2) or more copies of the proposal, the proposal may be rejected. However, if not rejected, the Master Copy will provide the basis for resolving such discrepancies.

Bidders should be sure that no pricing information of any type is shown in their proposal response, except in the sealed "Cost" envelope of the proposal, Volume 3. **The inclusion of pricing in any fashion or format in any other place in the proposal, except for the sealed cost data in the proposal, may result in immediate rejection of the proposal.**

As stated in subsection 2.4.5, Confidentiality, bidders should be aware that marking the Final Proposal "confidential" or "proprietary" may exclude it from consideration for award.

6.6 Final Proposal Format and Content

Each Volume of the proposal must be provided separately in a three-ring binder, submitted in the number of hard copies indicated in this section, and must be structured in the following manner:

6.6.1 Volume 1-Response to Administrative Requirements

1. Table of Contents

This Section must contain a Table of Contents. All major parts of the proposal, including forms, must be identified by volume and page number. The table of contents must identify all figures, charts, graphs, etc.

2. Responsibility Certification (Refer to subsection 3.5.2)

3. Cover Letter (Refer to Section 3.9)

4. Required solicitation Exhibits, in the Following Order:

- a. Exhibit 2: Intent to Bid form (if not already submitted)
- b. Exhibit 3: Confidentiality Statement (if not already submitted)
- c. Exhibit 4: Response to Administrative Requirements
- d. Exhibit 5: GSPD 05-105, Bidder Declaration
- e. Exhibit 6: Secretary of State Certification
- f. Exhibit 7: Workers' Compensation Certification
- g. Exhibit 8: Seller's Permit Certification
- h. Exhibit 9: Payee Data Record
- i. Exhibit 10: Iran Contracting Act of 2010
- j. Exhibit 11: Surety and other security documents (Not Applicable)

- k. Exhibit 12: DVBE Declarations
- l. Exhibit 13: Bidding Preferences and Incentives
- m. Exhibit 14: Commercially Useful Function Certification (CUF) Form
- n. Exhibit 15: TACPA Preference Request (Required if claiming TACPA Preference)
- o. Exhibit 16: List of Proposed Subcontractors (Public Works) (Not Applicable)
- p. Exhibit 17: Contractor's License Information (Not Applicable)

**Response to Qualification Requirements, and Solution Requirements. Required
Solicitation Exhibits, In The Following Order:**

- r. Exhibits 18.1 through 18.2: Bidder's Qualifications Form(s) and Bidder Reference Form(s)
- s. Exhibits 19.1 through 19.8: Staff Qualifications Forms and Staff Reference Forms
- t. Exhibit 20: Requirements Certification (MS) (Functional and Non-Functional Requirements)
- u. Exhibit 21: Proposal Narrative Requirements (MS)
- v. Exhibit 23: Bidders Library

6.6.2 Volume 2 - Contract

- 1. Exhibit 1: STD. 213, Standard Agreement
- 2. Statement of Work (Refer to Section 3.11)

6.6.3 Volume 3 - Cost

This volume must be in a separately sealed, marked envelope or container containing:
Exhibit 22 Cost Worksheet – Cost Table

7. EVALUATION

This section presents the evaluation process and scoring procedures the State will follow when evaluating proposals submitted in response to this solicitation. The evaluation process is multi-step, comprised of a thorough review of each bidder's proposal response to determine that it is responsive and responsible, and provides "best value" to the State. The value effective proposal is that proposal which meets all requirements set forth in this solicitation and offers the State the best combination of administrative, qualification, solution, and cost value as determined through the evaluation process specified in this section.

Final selection will be based on compliance with all requirements, seventy percent (70%)-scored solution requirements, and thirty percent (30%) cost among the bids that are responsive and responsible to the solicitation requirements. Responsiveness is comprised of meeting all bid requirements, and cost requirements, and conforming to the Rules Governing Competition in subsection 2.4 of the solicitation. Proposals that do not comply with the mandatory components stipulated in the solicitation may be deemed non-responsive and the bidder may be disqualified. The State reserves the right to cancel this procurement in its entirety at any time.

Bidders are required to thoroughly review all solicitation requirements to ensure that the proposal and the proposal responses are fully compliant with the solicitation requirements and thereby avoid the possibility of being ruled non-responsive. If the State finds that a final proposal has a material deviation from specified requirements, the proposal will be considered non-responsive and will not be considered for award.

7.1 EVALUATION TEAM

This procurement is being conducted under the guidance of a Procurement Official from the California Department of Technology, STPD (refer to subsection 2.2.1, Procurement Official). The Procurement Official will serve as the contact point with the bidder for questions and clarification, and will identify the rules governing this procurement.

STPD may engage additional qualified individuals or Subject Matter Experts (SME) during the evaluation process to assist the State in gaining a better understanding of technical, financial, legal, contractual, or program issues. These other individuals do not have voting privileges or responsibility for the evaluation process, but they will serve in an advisory capacity.

7.2 EVALUATION STEPS

7.2.1 Evaluation of Required Information and Requirements

Proposals must be complete and contain all requirements as identified Section 6, PROPOSAL/BID FORMAT AND SUBMISSION REQUIREMENTS. A final proposal may be rejected if it is conditional or incomplete. In addition, alteration of the solicitation or other irregularities of any kind including any terms and conditions by a bidder will result in rejection of the proposal.

A final proposal may be rejected if any such defect or irregularity constitutes a material deviation from the solicitation requirements.

7.2.1.1 Mandatory Requirements Evaluation

The State will review each proposal to determine its compliance with all of the requirements set forth in Section 3, ADMINISTRATIVE REQUIREMENTS and Section 4, BID REQUIREMENTS.

Each submitted proposal will be evaluated and scored by a consensus of the State Evaluation Team for compliance with the requirements designated in Section 4. If a Proposal fails to meet any of the requirements specified in Section 4, the State will determine if the deviation is material.

7.2.2 Receipt and Preliminary Review

All Proposals received by the time and date specified in subsection 2.3, KEY ACTION DATES, will be acknowledged as having been received at that time. Each proposal will be date and time marked as it is received and verified that all responses are submitted under an appropriate cover, sealed and properly identified. Proposals will remain sealed until the designated time for opening the bidders' Response, Volume 3 Cost Information, shall remain sealed and in the possession of the Procurement Official listed in subsection 2.2.1, until the evaluations of all bidder response volumes have been completed for all bidders submitting a proposal. The proposals will be checked by the Procurement Official for the presence of proper identification and the presence of required information, is in conformance with the proposal submittal requirements of Section 6, PROPOSAL/BID FORMAT AND SUBMISSION REQUIREMENTS. Absence of required information may make the proposal non-responsive and may result in bidder disqualification.

7.2.3 Validation against Requirements

The State will check each proposal in detail to determine its compliance to the solicitation requirements. The State reserves the right to determine if the bidder's response to a requirement, as detailed in their description and/or supporting documentation, supports or contradicts the bidder's claim of intended compliance. If a proposal fails to meet a Mandatory requirement, the State will determine if the deviation is material, as defined in subsection 2.4.1, IDENTIFICATION AND CLASSIFICATION OF SOLICITATION REQUIREMENTS. A material deviation is cause for rejection of the proposal. A material deviation cannot be waived.

During the evaluation of the bidder proposals, the State may request that the bidder clarify any area of the proposal that the State determined to be unclear. However, this request for clarification will not be an opportunity for the bidder to change their proposal.

7.4 Final Proposal Evaluation

The purpose of this section of the solicitation is to outline how the points will be awarded in a manner that preserves the integrity of the competitive procurement process. During proposal evaluation, failure to respond to a mandatory requirement is considered non-responsive and may be considered a material deviation. A material deviation will result in bidder disqualification.

The maximum points available for this solicitation are 1,000 points. All point calculations will be rounded to two (2) decimal places (the nearest hundredth). The Cost Data will only be opened if proposals are compliant to the Administrative, and Bid Requirements. Bidders that have a material deviation will be deemed non-responsive, disqualified and their cost data will not be opened. The distribution and allocation of maximum points possible for each proposal element is as follows:

Table 7-1: Scoring and Point Distribution

Maximum possible Scores for each Evaluation Area	
Section 3, ADMINISTRATIVE REQUIREMENTS	Pass/Fail
Section 4, BID REQUIREMENTS	Maximum Score 700
Bidder Qualification Forms	Pass/Fail
Bidder Reference Forms	Pass/Fail
Staff Qualification Forms	Pass/Fail
Staff Reference Forms	Pass/Fail
Exhibit 20 - Requirements Certification	Pass/Fail
Exhibit 21 – Proposal Narrative Requirements	700
Section 5, COST	Maximum Score 300
Cost Worksheets	300
Maximum Total Score	1,000

7.4.1 Errors in the Final Proposal

An error in the Final Proposal may cause the rejection of that proposal; however, the State may at its sole option retain the proposal and make certain corrections. In determining if a correction will be made, the State will consider the conformance of the proposal to the format and content required by the solicitation, and any unusual complexity of the format and content required by the solicitation.

1. If the bidder's intent is clearly established based on review of the complete final proposal submittal, the State may at its sole option correct an error based on that established intent.
2. The State may at its sole option correct obvious clerical errors.
3. The State may at its sole option correct discrepancy and arithmetic errors on the basis that if intent is not clearly established by the complete proposal submittal, the Master Copy shall have priority over additional copies, the proposal narrative shall have priority over the contract, the contract shall have priority over the cost sheets, and within each of these, the lowest level of detail will prevail. If necessary, the extensions and summary will be recomputed accordingly, even if the lowest level of detail is obviously misstated. The total price of unit-price items will be the product of the unit price and the quantity of the item. If the unit price is ambiguous, unintelligible, uncertain for any cause, or is omitted, it shall be the amount obtained by dividing the total price by the quantity of the item.
4. The State may, at its sole option, correct errors of omission, and in the following four situations, the State will take the indicated actions if the bidder's intent is not clearly established by the complete proposal submittal.
 - a. If an item is described in the narrative and omitted from the contract and cost data provided in the proposal for evaluation purposes, it will be interpreted to mean that the item will be provided by the bidder at no cost.
 - b. If a minor item is not mentioned at all in the Final Proposal and is essential to satisfactory performance, the proposal will be interpreted to mean that the item will be provided at no cost.
 - c. If a major item is not mentioned at all in the final proposal, the proposal will be interpreted to mean that the bidder does not intend to supply that item.
 - d. If a major item is omitted, and the omission is not discovered until after contract award, the bidder shall be required to supply that item at no cost. The determination of whether an item is minor or major is the responsibility of the State.
5. If a bidder does not follow the instructions for computing costs not related to the contract, if any, (e.g., State personnel costs), the State may reject the proposal, or at its sole option, re-compute such costs based on instructions contained in the solicitation.
6. If the re-computations or interpretations, as applied in accordance with this section, result in significant changes in the amount of money to be paid to the bidder (if awarded the contract) or in a requirement of the bidder to supply a major item at no cost, the bidder will be given the opportunity to promptly establish the grounds legally justifying relief from its proposal.

7. It is absolutely essential that bidders carefully review the cost elements in their final proposal, since they will not have the option to correct errors after the time for submittal of the Final Proposals.
8. The State may request clarification of items in the bidder's response if the meaning is not clear to the State. Responses to requests for clarification must be confirmed in writing by the bidder as instructed by the State's Procurement Official at the time of the request.
9. At the State's sole discretion it may declare the Final Proposal to be a Draft Proposal in the event that the State determines that Final Proposals from all bidders contain material deviations. Bidders may not protest the State's determination that all proposals have material deviations. If all proposals are declared noncompliant, the State may issue an addendum to the solicitation. Should this occur, the State may hold confidential discussions with participating bidders who are interested in continuing to be considered. Each participating bidder will be notified of the due date for the submission of a new Final Proposal to the State. This submission must conform to the requirements of the original solicitation as amended by any subsequent addenda. The new Final Proposals will be evaluated as required by Section 7, EVALUATION.

7.4.2 Rejection of Proposals

The State may reject any or all proposals and may waive any immaterial deviation or defect in a proposal. The State's waiver of any immaterial deviation or defect shall in no way modify the solicitation documents or excuse the bidder from full compliance with the solicitation specifications if awarded the contract.

7.4.3 Administrative Requirements (M, O)

Requirements in Section 3, ADMINISTRATIVE REQUIREMENTS labeled with (M) are mandatory, with the exception of subsection 3.19.2, Small Business Preference and subsection 3.19.5, Target Area Contract Preference Act (TACPA). Administrative Requirements in Section 3, labeled with (O) are Optional and bidders are not required to respond. Review of the detailed proposals will begin with ensuring that the bidder has responded to all administrative requirements, where indicated, in Section 3, for the appropriate proposal submittal documents.

Only Proposals passing the mandatory Administrative and Bid Requirements evaluation will proceed to cost opening. If a proposal fails to meet any of the Mandatory requirements specified in Section 3, ADMINISTRATIVE REQUIREMENTS, the State will determine if the deviation(s) is material. If the deviation is determined to be material, the proposal will be considered non-responsive and shall result in bidder disqualification.

7.4.4 Qualification Evaluation

All information submitted in the proposal will be evaluated in determining bidder and Staff Qualifications. Narrative descriptions on the Bidder Qualification Form, Exhibit 18.1, and Staff Qualification Forms, Exhibit 19.1 – 19.8, must be clear and apply directly to the relevant requirement. Narrative descriptions may be used to validate the other information on all forms. Any conflicting information may be deemed non-responsive and may result in the proposal being disqualified.

To aid the State in evaluating bidder and Staff Qualifications, bidders should use a MM/DD/YYYY format when indicating start and end dates for project history on Exhibit 18.1 Bidder Qualification Form, and Exhibits 19.1 – 19.8, Staff Qualification Forms. If a bidder submits a proposal in any other format, the State will count only the whole months or years between the start and end dates. For example, bidder “A” cites a start and end date for Project 1 as 6/2011 to 12/2011. The bidder would only be credited with five (5) months of experience.

If a project end date or experience end date identified on the Bidder/Staff Qualification forms exceeds the Final Proposal due date (for an on-going project) then the bidder will receive credit for only the experience acquired up to the Final Proposal due date.

If the number of years for a specific experience requirement was not indicated on the Bidder/Staff Qualification forms and the bidder/staff checked “yes” to meeting a minimum requirement then the bidder/staff will receive credit for only the minimum number of years required for that requirement or will receive the number of years indicated on the form header, whichever is less.

7.4.4.1 Bidder Qualifications

The State will evaluate the bidders qualifications using the information contained in Exhibit 18.1. Bidders must provide for at least three (3) projects and not more than six (6) projects. Bidders must submit one (1) completed form for each of the projects cited. Bidders who do not return the required Qualification Forms shall be deemed non-responsive.

Each submitted form will be evaluated for compliance with the requirements specified in subsection 4.1.1, Bidder Qualifications and in accordance with the criteria set forth in Exhibit 18.1. If any submitted form fails to adequately document the bidder experience and how it meets the requirements, the State will determine if the deviation is material. If the deviation is determined to be material, the proposal will be considered non-responsive.

7.4.4.2 Bidder References

The State will evaluate the bidder’s references using the information provided in Exhibit 18.2.

Each bidder Reference Form must be signed by a client reference contact that performed an oversight role on the referenced project.

All reference forms must be returned with the proposal submittal in order to meet the bidder minimum experience requirements. Bidders who do not return the required Reference Forms shall be deemed non-responsive.

If the Client reference is not allowed either legally or by company/organization policy to sign the Client reference form, the Client reference must type in their full name with a brief statement on the form outlining the reason they are not permitted to sign the States reference form. If needed, the State may contact either the Bidder and/or Staff References to validate the reference submitted. The State will make two (2) attempts via email to validate Bidder and/or Staff experience using the information provided in the Bidder and/or Staff Reference forms, as applicable.

Reference scores will be calculated by totaling the ratings from each reference form submitted. All bidder reference form points will be totaled. The Bidder must obtain sixty-five percent (65%) of the maximum possible bidder reference points available to pass. The maximum possible points will vary depending on the number of reference forms submitted. Example, if a bidder submits five (5) reference forms, the maximum possible points will be ninety (90) points. The bidder must obtain sixty-five percent (65%) out of ninety (90) points to pass, which is fifty-eight and a half points (58.5).

7.4.4.3 Staff Qualifications

The State will evaluate the bidder's staff experience using the information provided in Exhibit 19.1 through 19.8. If any information on the form(s) fails to meet any of the experience requirements, the State will determine if the deviation is material. If the deviation is determined to be material, the proposal will be deemed non-responsive and the bidder will be disqualified.

Reference contacts listed on attachments may be contacted to verify information provided by the bidder.

7.4.4.4 Staff References

The State will evaluate the bidder's staff references using the information provided in Exhibits 19.1 through 19.8.

All reference forms must be returned with the proposal submittal in order to meet the Staff Reference requirements. One (1) reference form must be submitted for every project cited on Exhibit 19 through 19.8. Bidders who do not return the required Reference Forms shall be deemed non-responsive.

Each staff Reference Form must be signed by a client reference contact that performed a technical or supervisory role on the referenced project. References must be returned with the proposal submittal in order to meet the Staff Reference requirements. Bidders who do not return the required Reference Forms shall be deemed non-responsive and the bidder shall be disqualified.

If the client reference is not allowed either legally or by company/organization policy to sign the client reference form, the client reference must type in their full name with a brief statement on the form outlining the reason they are not permitted to sign the States reference form. If needed, the State may contact either the Bidder and/or Staff References to validate the reference submitted. The State will make two (2) attempts via email to validate Bidder and/or staff experience using the information provided in the Bidder and/or Staff Reference forms, as applicable.

Reference scores will be calculated by totaling the ratings from each reference form submitted. All staff reference form points will be totaled. The Bidder must obtain sixty-five percent (65%) of the maximum possible bidder reference points available to pass. The maximum possible points will vary depending on the number of reference forms submitted. Example, if a bidder submits five (5) reference forms, the maximum possible points will be ninety (90) points. The bidder must obtain sixty-five percent (65%) out of ninety (90) points to pass, which is fifty-eight and a half points (58.5).

7.4.4.5 Bidder and Staff Client Reference Checks

If needed to verify either the bidder or staff's qualifications, the State will make two (2) attempts via email to validate the bidder's or staff's experience using the information provided in the Bidder and/or Staff Reference Forms. Bidders should ensure that references are available for validation during the evaluation period identified in subsection 2.3, KEY ACTION DATES.

If the State has not received a response from the bidder or staff's Referenced Contact after the first attempt, a second attempt will be made. If no response is received after the second attempt, the State will contact the bidder and request that the bidder assist the State by having the reference respond to the State within a 48-hour period from the second attempted contact. If the evaluators are still unable to contact the reference(s), the bidder may be deemed non-responsive for failure to provide verifiable references.

7.4.5 Functional and Non-Functional Requirements Evaluation

The Functional and Non-Functional Requirements are identified in Exhibit 20 SOW and consist of Mandatory (M) requirements. Bidders must provide a complete response to each

requirement, as described in subsection 4.2.1, Contractor Requirements. The Evaluation Team will evaluate these requirements on a pass/fail basis.

7.4.6 Narrative Response(s) Evaluation – Exhibit 21

The Evaluation Team will evaluate the response to each proposal response requirement to determine whether the response fully addresses the requirements in accordance with the evaluation criteria set forth in Table 7.2, Proposal Narrative Requirements and Mandatory Scorable Response Requirements Evaluation Criteria. The Evaluation Team will evaluate each proposal response based on the evaluation criteria of the three characteristics identified in Table 7.2.

Table 7.2 Proposal Narrative Requirements Evaluation Criteria Table

Characteristic	Evaluation Criteria and Points			
	3 - Excellent	2 - Good	1 - Fair	0 - Poor
A Comprehension The extent to which the Bidder's response demonstrates its understanding of the requirement	Response clearly demonstrates a thorough understanding of all aspects of the RFP requirement. Timely and high quality performance is anticipated.	Response clearly demonstrates a thorough understanding of most aspects of the RFP requirement. Timely and high quality performance is anticipated.	Response demonstrates an understanding of some aspects of the RFP requirement. Timely and acceptable quality performance is anticipated.	Response lacks an understanding of the RFP requirement. Timely and acceptable quality performance is doubtful.
B Quality The quality of the Bidder's response, including consistency with industry standards	Approach, methods, tools, or deliverables are appropriately tied throughout all of the relevant areas. Underlying principles of the relevant areas are consistent with the overall approach.	Approach, methods, tools, or deliverables are appropriately tied throughout most of the relevant areas. Underlying principles of most relevant areas are consistent with the overall approach.	Approach, methods, tools, or deliverables are minimally tied throughout the relevant areas. Underlying principles of some relevant areas are consistent with the overall approach.	Approach, methods, tools, or deliverables are not tied to a relevant area. Underlying principles of that relevant area are inconsistent with the overall approach.
C Value The level to which the response provides benefit and value to the State, while not increasing risk	Response contains major strengths, exceptional functionalities that substantially exceed the requirement. Response contains an extremely high level of automation. There are no weaknesses or deficiencies. Risk of failing	Some strengths, exceptional functionalities, exceed the requirement. Response contains a high level of automation. There are very few weaknesses or deficiencies. Weaknesses, if any, are minor and are more than offset by the strengths.	There are minor strengths, functionalities, that satisfy the requirement. Response contains some automation. Contains minor weaknesses, slight inconsistencies, or deficiencies. Weaknesses are generally offset by any strength. Risk of failing to	There are no strengths, functionality, and does not meet the requirement. Response lacks automation. Contains major weaknesses, inconsistencies, and deficiencies. Weaknesses are not

State of California
Office of Systems Integration

RFP OSI 31326
Part 1 – General Instructions
December 21, 2015

Characteristic	Evaluation Criteria and Points			
	3 - Excellent	2 - Good	1 - Fair	0 - Poor
	to deliver this requirement is extremely low.	Risk of failing to deliver this requirement is low.	deliver this requirement is moderate.	offset by strengths. Risk of failing to deliver this requirement is very high.

Each characteristic will be evaluated separately and awarded a maximum rating of 3, for a maximum available rating of 9, for each proposal response requirement. The rating earned per requirement will then be divided by the maximum available rating of 9 and rounded to the nearest hundredth. The resulting percentage is the Bidder's "response rating factor," which is then multiplied by the maximum available points per proposal response requirement to arrive at the Bidder's awarded points. Table 7.3 - Bidder Proposal Response Requirement Score Calculation Example illustrates how each proposal response requirement will be scored. The Bidder's overall Proposal Response Requirements Score will be the cumulative total of the Bidder's scores for all proposal response requirements.

Table 7.3 Bidder Proposal Response Requirement Score Calculation EXAMPLE

Req. #	Calculation							= Proposal Response Score (per requirement)*				
	Comp. Rating	+	Quality Rating	+	Value Rating	=	Bidder Total Rating	÷ Max Rating	=	Response Rating Factor*	× Max Avail Points Per Req.	
1	3		2		2		7	9		.78	90 Points	70.2

* Rounded to the nearest hundredth

7.4.7 DVBE Incentive

In accordance with §999.5(a) of the Military and Veterans Code, for evaluation purposes only, the State shall provide an incentive to bidders who provide California-certified DVBE participation that exceeds the mandatory California-certified DVBE participation goal in the amounts shown in Table 7.3 – DVBE Participation Incentive Formula.

The State will verify DVBE and apply the incentive accordingly. The DVBE Incentive points are a percentage of the total possible points. The maximum incentive for this procurement is five percent (5%) of the total points available, and is based on the amount of DVBE participation confirmed. The below table is an illustration of this calculation:

Table 7.4 – DVBE Participation Incentive Formula

Confirmed DVBE Participation	DVBE Incentive Percentage (% of total points available)	DVBE Incentive Points
>= 5%	5%	50.00 (1,000 x 0.05)
4% - 4.99%	4%	40.00 (1,000 x 0.04)
3-3.99%	3%	30.00 (1,000 x 0.03)

7.4.8 Cost Evaluation

After the Administrative and Bid Requirements are evaluated, the cost information (bidder's Response to Volume 3) will be opened for those bidders whose proposals have been deemed responsive and responsible. Those cost proposals will be validated to verify that the cost worksheets are complete and free of mathematical errors. If appropriate, errors will be corrected in accordance with subsection 7.4.1.

Cost Information (bidder's Response to Volume 3) will not be opened until the State has completed its evaluation of the Administrative, and Bid requirements. Bidders whose proposals have been determined to be responsive and responsible will have their sealed Cost Information opened. If a bidder was determined to be non-responsive and/or not responsible during the evaluation of the Administrative, Bid Requirements and the Cost Information will remain unopened for that bidder.

NOTE: If a bidder's Cost Information fails to meet the requirement to be submitted under separate, sealed cover, the State may immediately deem the bidder's proposal to be non-responsive and may discontinue evaluation of the proposal.

All cost worksheets will be checked for mathematical accuracy. After costs workstation have been verified for accuracy, the bidder with the lowest Proposed Total Cost will receive the maximum score of 300 points. All other bidders will receive a proportionally lower score that is the ratio of the lowest proposed total cost to the bidder's Proposed Total Cost, applied to the maximum points of 300 using the following bidder Cost Score Formula below:

Table 7.5– Bidder Cost Score Formula

Bidder Cost Score Formula
$\frac{(\text{Lowest Proposed Total Cost})}{(\text{Bidder's Proposed Total Cost})} \times 300 \text{ Points} = \text{Bidder Cost Score}$

In the Bidder's Cost Score Calculation Example below, Bidder C proposed the lowest cost:

Table 7.6 – Bidder Cost Score Calculation

Bidder Cost Score Calculation			
Bidder	Bidder's Proposed Total Cost	Calculation	Bidder Cost Score
A	\$500,000	\$300,000 \$500,000 X 300 points	180 points
B	\$400,000	\$300,000	225 points
		\$400,000 X 300 points	
C	\$300,000	\$300,000 \$300,000 X 300 points	300 points

NOTE: The numbers in this table are used for illustration purposes only and do not represent any expectation on the part of the State.

7.4.9 Preference Programs

Bidders who claim preference points will be evaluated to determine whether they submitted the forms, documents, exhibits, and/or responses necessary to validate their qualification and eligibility for the claimed points. If the State determines that the submitted information is insufficient, or that required documents do not otherwise validate the eligibility for points in any of the claimed programs, then the claimed points for that program will not be added to the bidder's final overall proposal score. If the State is able to validate the bidder's claim, the qualified preference points will be applied to the bidder's final overall proposal score as illustrated in Table 7.9, Final Proposal Score with Small Business provided that the bidder's proposal is not otherwise determined to be non-responsive to any Mandatory requirements.

7.4.9.1 Small Business Preference

The State will verify Small Business / Non-Small Business preference claim and apply the five percent (5%) preference accordingly.

Per Government Code §14835 et seq., bidders who qualify as a small business will be given a five percent (5%) preference for evaluation purposes only. The five percent (5%) preference is calculated on the total number of points awarded to the highest scoring non-small business that is responsible and responsive to the proposal requirements. The rules and regulations of this law, including the definition of a small business for the delivery of goods and services, are contained in the California Code of Regulations, Title 2, § 1896 et seq.

This five percent (5%) small business preference is also available to a non-small business claiming 25% California certified small business subcontractor participation. The five percent (5%) preference is calculated on the total number of points awarded to the highest scoring non-small business that is responsible and responsive to the proposal requirements and that is not subcontracting a minimum of 25% to a small business. Non-small business bidders claiming the five percent (5%) small business preference must commit to subcontract at least 25% of the net proposal price with one (1) or more California certified small businesses.

Completed certification applications and required support documents must be submitted to the Office of Small Business and DVBE Services (OSDS) no later than 5:00 p.m. on the Final Proposal due date, and the OSDS must be able to approve the application as submitted. Questions regarding certification should be directed to the OSDS at (916) 375-4940.

For an illustration of this process, refer to Table 7.7 - Small Business Preference Points Calculation Example. Points in this example explain the calculations and have no other significance.

The Preference Points for bidders A and B are based on five percent (5%) of the bidder proposal Score of Bidder C, the highest scorer of a non-small business, which is $(650.00 \text{ points}) \times (.05) = 32.50 \text{ points}$ (rounded). Bidder C, which is neither a small business nor a non-small business subcontracting a minimum of 25 percent (25%) to a small business, receives no Small Business Preference Points.

Table 7.7 – Small Business Preference Points Calculation

Small Business Preference Points Calculation				
Bidder	Bidder Total Proposal Score	Small Business Preference Claim?	Non-Small Business Preference Claim?	Small Business Preference Points Awarded
A	700 pts	Yes	No	35 pts
B	700 pts	No	Yes	35 pts
C	650 pts	No	No	0 pts

NOTE: Calculation is based on 5% of the bidder with the highest “Bidder Proposal Score” that is a non-small business. In the example above, Bidder C has the highest non-small business score.

7.4.9.2 TACPA Preference

The State will verify TACPA and apply the preference accordingly.

Table 7.8 – TACPA Preference

Bidder	Bidder Proposal Total Score	TACPA Preference %	Preference Given
A	700 pts	5.00%	42.50 pts
B	700 pts	0.00%	0.00 pts
C	650 pts	0.00%	0.00 pts

7.4.10 Bidder Final Score Calculation and Rank Determination

The Evaluation team will calculate the Bidder's Final Score. Table 7.9 below illustrates the Bidder's Final score that encompasses both preference and incentive points:

Table 7.9 – Bidder Final Score Calculation

Bidder Final Score Calculation						
Bidder	Bidder Proposal Total Score	Small Business Preference Points Awarded	Verified DVBE %	DVBE Points Awarded	TACPA Preference %	Bidder Final Score
A	700.00 pts	35 pts	3%	21 pts	42.50 pts	798.50 pts
B	700.00 pts	35 pts	4%	28 pts	0.00 pts	763 pts
C	650.00 pts	0.00 pts	5%	32.50 pts	0.00 pts	682.50 pts

NOTE: Bidder Final Score Calculation above is an example that explains the calculations and has no other significance.

7.4.11 Selecting the Proposed Awardee

Award of contract, if made, will be to a responsible bidder whose Final Proposal complies with all the requirements of the solicitation and any addenda thereto, except for such immaterial defects as may be waived by the State, and whose proposal achieves the highest number of total points for requirements, references, cost, and any preferences and/or incentives.

The State will determine which bidders are responsive and responsible. The State will determine which bidder has the highest combined score for the Bid Requirements and cost, up to the maximum points, plus any preference and/or incentive points. The State will rank all

qualified proposals by the bidder's Final Score and then recommend the bidder with the highest bidder Final Score to be the proposed awardee. Table 7.10 below demonstrates how the final ranking determination is made:

Table 7.10 – Final Score and Rank Determination

Final Score and Rank Determination				
Scoring Element	Max Points Available	Bidder A	Bidder B	Bidder C
Narrative Response Requirements	700	700	700	650
Cost Score	300	150	175	100
Total Proposal Score	1000	850	875	750
Initial Rank (Before Preferences and Incentives)		2	1	3
Small Business Preference Points	50	42.5	43.75	0
DVBE Incentive Points	50	25.50	35	37.50
TACPA Preference Points	50	42.5	0	0
Bidder Final Score	1150	960.50	953.75	787.50
Final Rank		1	2	3

7.5 NEGOTIATIONS

The State of California reserves the right to negotiate. Should it be determined that it is in the State's best interest, the State will conduct negotiations under PCC §6611. The purpose of the negotiations is to maximize the State's ability to obtain value effective, based on the requirements and the evaluation factors set forth in the solicitation.

Negotiations allow the State and bidder an opportunity to discuss items that could, in the State's opinion enhance the bidder's proposal and potential for award. Negotiations are not intended to allow a bidder to completely rewrite their proposal. The negotiations are exchanges between the State and the bidder, which are undertaken with the intent of allowing the bidder to revise their Final Proposal only in areas determined by the State during the negotiations. Negotiations will be conducted either orally or in writing. These negotiations may include bargaining, such as persuasion, alteration of assumptions and positions.

The State may discuss any aspect of the bidder's proposal that could, in the opinion of the State, be altered or explained to materially enhance the proposal's potential for award. However, the State is not required to discuss every area where the bidder's proposal could be

improved. The scope and extent of negotiation exchanges are the matter of the State's judgment.

All aspects of the Bidder's proposal are confidential until after the issuance of the Notification of Award.

7.5.1 Proceeding to Negotiations

At the discretion of the State, the top three (3) highest scoring compliant bidders will be determined eligible to participate in the negotiations. At the discretion of the State, the State may invite bidder(s) to participate in the negotiations under the following:

The State will invite and proceed with negotiations with the top highest scoring compliant Bidder and may be awarded a contract. If the State cannot come to an agreement with the top highest scoring compliant Bidder, the State will determine the bidder disqualified and will invite and proceed with negotiations with the next highest scoring compliant Bidder. This bidder negotiation selection process will continue until the State completes negotiations with the final selected bidder and may be awarded a contract.

7.5.2 Negotiation Invitation

Once compliant bidders are determined those bidders will be notified in writing: (1) that the State is initiating negotiations pursuant to Public Contract Code 6611(a); (2) the general purpose and scope of the negotiations; (3) the anticipated schedule for the negotiations; and (4) the procedures to be followed for negotiations.

At the discretion of the State, the State may invite bidder(s) to participate in the negotiations stated previously in negotiations subsection 7.5.1:

Confirmation of Attendance: Bidder(s) who have been invited to participate in negotiations must confirm attendance, in accordance with the invitation instructions, within two (2) State business days of invitation.

7.5.3 Best and Final Offer Submission (BAFO)

At the conclusion of negotiations, the State may request a Best and Final Offer (BAFO) submission. The intent of the BAFO is to clarify and document understandings reached during negotiations. The State will establish a date and time for receipt of the BAFOs based on when the bidder's BAFO negotiations occur. A bidder's BAFO is an irrevocable offer for 180 calendar days following the scheduled date for Submission of a Final Accepted BAFO. A bidder may extend the offer in the event of a delay in contract award.

BAFOs must be submitted to the location identified in subsection 2.2.1, Procurement Official, by the specific date and time that will be communicated to each bidder individually in writing.

The BAFO submission must address the following:

1. A supplemental proposal containing every negotiated/revised section(s) of the bidder's original final proposal, any other revised area specifically required by the State to be included in the BAFO, and revisions made necessary in accordance therewith.
2. The supplemental proposal must include all changes made to negotiated section(s) of the bidder's original Final Proposal in tracked changes. Changes to the bidder's original final proposal that are not tracked in the supplemental proposal or otherwise identified, may result in rejection of the proposal or cause for termination of the contract.
3. An executive summary must accompany the supplemental proposal, identifying a list of all changes (other than non-substantive changes to formatting, punctuation and grammar) that have been made to the bidder's original final proposal. The bidder must include and attest to the following statement within the executive summary:

"This Best and Final Offer (BAFO) is in response to {RFP OSI 31326} and the changes identified in this executive summary represent all changes made to {bidder's name} Final Proposal previously submitted to the State. Any substantive change not included in this list is non-operative, non-binding and will not be considered a part of the {bidder's name} BAFO."

7.5.4 Evaluation of BAFO Submission

The State will evaluate the BAFO submissions, based on topics negotiated. The State will document the evaluation process in accordance with the evaluation selection criteria outlined in the negotiation invitation letter.

7.5.5 Selection

Upon completion of evaluation of the BAFOs, final selection will be determined on the responsive and responsible bidder submitting the highest scoring (after preferences and incentives) supplemental proposal. The State reserves the right at any time to reject any or all proposals.

7.5.6 Debriefing

A debriefing may be held after contract award at the request of any bidder for the purpose of receiving specific information concerning the evaluation. The discussion will be based primarily on the Qualifications and Solution Requirements and cost evaluations of the Bidder's Final Proposal. A debriefing is not the forum to challenge the solicitation specifications or requirements.

8. INFORMATIONAL ATTACHMENTS

The following attachments to this solicitation are informational for use in the solicitation process and may not need to be submitted with the bidder's solicitation response. They can be found in Part 2, bidder's response:

1. Attachment 1 - Template for Question Submittal. This attachment provides the format for which a bidder shall submit questions regarding this solicitation.
2. Attachment 2 - Template for Request for Changes Submittal. This attachment provides the format for which a bidder shall submit requests for changes to this solicitation.
3. Attachment 3 - Procedures for conducting protests under the Alternative Protest Process.
4. Attachment 4 - Proposal Submission Checklist. This attachment references items to be submitted as part of the Final Proposal Submission, but is not guaranteed to include all necessary items.



REQUEST FOR PROPOSAL (RFP)

RFP #31326

PART 2 – BIDDER'S RESPONSE

FOR

Child Welfare Services – New System (CWS-NS) Application Program Interface (API)

December 21, 2015

Issued by:

STATE OF CALIFORNIA

Issued by:

STATE OF CALIFORNIA

Department of Technology

Statewide Technology Procurement Division

10860 Gold Center Drive

Rancho Cordova, CA 95670

In conjunction with:

STATE OF CALIFORNIA

Office of Systems Integration

2525 Natomas Park Drive, Suite 200

Sacramento, CA 95833

Part 2 of the solicitation contains all forms the bidders must complete and return with their proposals; including the STD 213, SOW, administrative forms, qualification forms, requirement responses and all Exhibits/Attachments discussed in Part 1.

Disclaimer: The original PDF version and any subsequent addendums of the RFP released by the Procurement Official of this bid remain the official version. In the event of any inconsistency between the Bidder's versions, articles, attachments, specifications or provisions which constitute the Contract, the official State version of the RFP in its entirety shall take precedence.

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

**RFP
PART 2
BIDDER RESPONSE**

TABLE OF CONTENTS

EXHIBIT A STATEMENT OF WORK	1
EXHIBIT 1: STD 213, STANDARD AGREEMENT	2
EXHIBIT 2: INTENT TO BID.....	3
EXHIBIT 3: CONFIDENTIALITY STATEMENT	4
EXHIBIT 4: RESPONSE TO ADMINISTRATIVE REQUIREMENTS	0
EXHIBIT 5: GSPD 05-105 BIDDER DECLARATION	2
EXHIBIT 6: SECRETARTY OF STATE CERTIFICATION.....	4
EXHIBIT 7: WORKERS’ COMPENSATION CERTIFICATION.....	6
EXHIBIT 8: SELLER’S PERMIT CERTIFICATION.....	8
EXHIBIT 9: PAYEE DATA RECORD.....	10
EXHIBT 10: IRAN CONTRACTING ACT OF 2010.....	12
EXHIBT 12: DVBE DECLARATIONS.....	16
EXHIBIT 13: BIDDING PREFERENCES AND INCENTIVES	18
EXHIBIT 14: COMMERCIALLY USEFUL FUNCTION (CUF) CERTIFICATION	20
EXHIBIT 15: STD 830 TACPA PREFERENCE REQUEST	22
EXHIBIT 16: LIST OF PROPOSED SUBCONTRACTORS (PUBLIC WORKS) *(NOT APPLICABLE)	24
EXHIBIT 17: CONTRACTOR’S LICENSE INFORMATION *(NOT APPLICABLE). 26	26
EXHIBIT 18: BIDDER QUALIFICATION FORM - INSTRUCTIONS	28
EXHIBIT 18.1: BIDDER QUALIFICATIONS FORM.....	29
EXHIBIT 18.2: BIDDER REFERENCE FORM.....	33
EXHIBIT 19: STAFF QUALIFICATIONS FORM INSTRUCTIONS	35
EXHIBIT 19.1: MANAGEMENT LEAD/ACCOUNT REPRESENTATIVE QUALIFICATIONS FORM	36
EXHIBIT 19.2 MANAGEMENT LEAD/ACCOUNT REPRESENTATIVE - REFERENCE FORM.....	38
EXHIBIT 19.3: LEAD DEVELOPER QUALIFICATIONS FORM	40

EXHIBIT 19.4: LEAD DEVELOPER - REFERENCE FORM.....	42
EXHIBIT 19.5: SCRUM MASTER QUALIFICATIONS FORM	44
EXHIBIT 19.6: SCRUM MASTER - REFERENCE FORM.....	46
EXHIBIT 19.7: PRODUCT DEVELOPMENT TEAM QUALIFICATIONS FORM.....	47
EXHIBIT 19.8: PRODUCT DEVELOPMENT TEAM - REFERENCE FORM	49
EXHIBIT 21: PROPOSAL NARRATIVE REQUIREMENTS (MS)	53
EXHIBIT 22: COST WORKSHEETS	55
EXHIBIT 23: BIDDERS’ LIBRARY ACCESS AUTHORIZATION FORM	57
ATTACHMENT 1 – TEMPLATE FOR QUESTION SUBMITTAL.....	59
ATTACHMENT 2 – TEMPLATE FOR REQUEST FOR CHANGES SUBMITTAL ..	61
ATTACHMENT 3: PROCEDURES FOR CONDUCTING PROTESTS UNDER THE ALTERNATIVE PROTEST PROCESS.....	63
ATTACHMENT 4 – SOLICITATION SUBMISSION CHECKLIST	73

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015

EXHIBIT A STATEMENT OF WORK

Please see Exhibit A – Statement of Work

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

EXHIBIT 1: STD 213, STANDARD AGREEMENT

**STATE OF CALIFORNIA
STANDARD AGREEMENT
STD. 213 (REVISED 07/12)**

REGISTRATION NUMBER:

PURCHASING AUTHORITY
NUMBER:

AGREEMENT NUMBER:

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

STATE AGENCY'S NAME

CONTRACTOR'S NAME

2. The term of this mm/dd/yyyy through mm/dd/yyyy or upon STPD approval, whichever is later
Agreement is:

3. **The maximum amount if \$
this Agreement is:**

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

CWS-NS General Provisions – Information Technology

Exhibit A, Statement of Work (includes Special Provisions and Definitions)

Exhibit 22, Cost Worksheets

Exhibit 21, Proposal Narrative Requirements Response

(*)RFP 31326 in its entirety

(*) Contractor's Final Proposal RFP 31326 in its entirety

Items shown with an Asterisk (), are hereby incorporated by reference and made part of this agreement as if attached hereto. Exhibit 23: Bidders Library contents can be viewed upon written request to the State Procurement Official.*

IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto.

	Use Only
CONTRACTOR	
CONTRACTOR'S NAME (If other than an individual, state whether a corporation, partnership, etc.)	
BY (Authorized Signature) 	DATE SIGNED
PRINTED NAME AND TITLE OF PERSON SIGNING	
ADDRESS	
STATE OF CALIFORNIA	
AGENCY NAME	
BY (Authorized Signature) 	DATE SIGNED
PRINTED NAME AND TITLE OF PERSON SIGNING	
ADDRESS	
	<input type="checkbox"/> Exempt per

EXHIBIT 2: INTENT TO BID

Department of Technology
Statewide Technology Procurement Division
P. O. BOX 1810, MS Y12
Rancho Cordova, CA 95741
Phone: 916-431-5558
E-mail address: becky.fatur@state.ca.gov

We: (select one)

- Intend to submit a bid and has no problem with the solicitation requirements.
- Intend to submit a bid, but has one or more problem(s) with the requirements for the reason(s) stated below.
- Does not intend to submit a bid for reason(s) stated below and has no problem with the solicitation requirements:
- Does not intend to submit a bid for reason(s) stated below and has one or more problem(s) with the solicitation requirements:

The individual to whom all information regarding this solicitation shall be transmitted is:

Name:			
Address:			
City, State and ZIP Code:			
Telephone:		FAX:	
E-Mail:			

Sincerely,

Name (Signature) _____ **Name and Title** _____ **Email** _____

_____ **Company** _____ **Telephone** _____ **FAX** _____

EXHIBIT 3: CONFIDENTIALITY STATEMENT

As an authorized representative and / or corporate officer of the company named below, I agree that all persons employed by this company will adhere to the following policy:

All information belonging to the Department of Technology or its affiliated agencies is considered sensitive and / or confidential and cannot be disclosed to any person or entity that is not directly approved to participate in the work required to execute this Agreement.

I certify that I will keep all project information, including, but not limited to information concerning the planning, processes, development or procedures of the Project, and all communication with Department of Technology or its affiliates derive of any procurement process, confidential and secure. I will not copy, give or otherwise disclose such information to any other person unless the Department of Technology has on file a Confidentiality Statement signed by the other persons, and the disclosure is authorized and necessary for the Project. I understand that the information to be kept confidential includes, but is not limited to, specifications, administrative requirements, terms and conditions, concepts and discussions, as well as written and electronic materials. I further understand that if I leave this project before it ends, I must still keep all project information confidential. I agree to follow any instructions provided by the Project relating to the confidentiality of project information.

I fully understand that any unauthorized disclosure I make may be basis for civil or criminal penalties and / or disciplinary action (for state employees). I agree to advise the contract manager immediately in the event of an unauthorized disclosure, inappropriate access, misuse, theft or loss of data.

All materials provided for this Project, except where explicitly stated will be promptly returned or destroyed, as instructed by an authorized Department of Technology representative. If the materials are destroyed and not returned, a letter attesting to their complete destruction which documents the destruction procedures must be sent to the contract manager at the Department of Technology before payment can be made for services rendered. In addition, all copies or derivations, including any working or archival backups of the information, will be physically and / or electronically destroyed within five (5) calendar days immediately following either the end of the contract period or the final payment, as determined by the Department of Technology.

All personnel assigned to this project shall be provided a Confidentiality Statement and will be expected to sign and return it to the representative listed below before beginning work on this project.

Representative Name:		Title:		Phone Number:	
Company Name:					
Address:					
City/State/Zip Code:					
Signature:					
Date:					

EXHIBIT 4: RESPONSE TO ADMINISTRATIVE REQUIREMENTS

Bidder shall indicate agreement to each of the Administrative Requirements as presented in Section 3 of Part I in the Table below. By indicating “Yes” the Bidder affirms that it understands the requirement and agrees to comply with it.

RFP Section*	Administrative Requirement –RFP Section 3	Bidder Agrees Y / N
	Administrative Requirements (M)	
3.1	Ability to Perform	
3.2	Primary Bidder	
3.3	Subcontractors	
3.3.1	Bidder Declaration Form (M)	
3.4	Amendment	
3.5	Responsibility Certification (M)	
3.6	CWS-NS General Provisions - Information Technology	
3.7	Commercial General Liability Insurance	
3.8	Administrative Requirements Document (M)	
3.9	Cover Letter (M)	
3.10	STD 213, Standard Agreement (M)	
3.11	Statement of Work (SOW) (M)	
3.12	Confidentiality Statement (M)	
3.13	Secretary of State (M)	
3.14	Worker’s Compensation (M)	
3.15	Seller Permit (M)	
3.16	Payee Data Record (Std. 204) (M)	
3.17	Iran Contracting Act of 2010 (M)	
3.18.1	Disabled Veteran Enterprise (DVBE) Program	

**State of California
Office of Systems Integration**

**RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015**

3.18.1.1	DVBE Participation Requirement (M)	
3.18.1.2	DVBE Participation Incentive (M)	
3.18.2	Small Business Preference (O)	
3.18.3	Non-Small Business Preference (O)	
3.18.4	Commercially Useful Function (M)	
3.18.5	Target Area Contract Preference Act (TACPA) (O)	
3.19	Productive Use Requirements	
3.19.1	Customer In-use	
3.19.2	Customer References for Productive Use Requirements (M)	
3.19.3	Equipment	
3.20.1	Labor	
3.20.2	Travel and Subsistence Payments	
3.20.3	Apprentices	
3.20.4	Payroll	

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

EXHIBIT 5: GSPD 05-105 BIDDER DECLARATION

A copy of the *GSPD-05-105 Bidder Declaration* and its instructions is available as a fill and print PDF at:
<http://www.documents.dgs.ca.gov/pd/poliproc/Master-Biddeclar08-09.pdf>

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015

EXHIBIT 6: SECRETARY OF STATE CERTIFICATION

ATTACH A COPY OF THE BIDDERS SECRETARY OF STATE CERTIFICATION TO THIS EXHIBIT.

For more information on seller's permit or certification of registration, refer to the following website link:
<http://kepler.sos.ca.gov/>

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

EXHIBIT 7: WORKERS’ COMPENSATION CERTIFICATION

The undersigned in submitting this document hereby certifies the following:

I am aware of the provisions of Section 3700 of the California Labor Code which requires every employer to be insured against liability for workers’ compensation or to undertake self-insurance in accordance with such provisions before commencing the performance of the work of this contract.

Signature

Date

Name and Title (Print or Type)

Street Address

Firm Name

City, State, ZIP

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

EXHIBIT 8: SELLER’S PERMIT CERTIFICATION

ATTACH A COPY OF THE BIDDERS CALIFORNIA SELLERS PERMIT TO THIS EXHIBIT.

For more information on seller’s permit or certification of registration, refer to the following link:
<http://boe.ca.gov/pdf/pub73.pdf>

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015

EXHIBIT 9: PAYEE DATA RECORD

ATTACH A COPY OF THE BIDDERS STD 204, PAYEE DATA RECORD TO THIS EXHIBIT.

Refer to the following website link to obtain the appropriate form. Payee Data Record (STD 204) for information: <http://www.documents.dgs.ca.gov/dgs/fmc/pdf/std204.pdf>

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

EXHIBIT 10: IRAN CONTRACTING ACT OF 2010**IRAN CONTRACTING ACT**

(Public Contract Code § 2202-2208)

Prior to bidding on, submitting a proposal or executing a contract or renewal for a State of California contract for goods or services of \$1,000,000 or more, a vendor must either: a) certify it is not on the current list of persons engaged in investment activities in Iran created by the California Department of General Services (“DGS”) pursuant to Public Contract Code § 2203(b) and is not a financial institution extending twenty million dollars (\$20,000,000) or more in credit to another person, for 45 days or more, if that other person will use the credit to provide goods or services in the energy sector in Iran and is identified on the current list of persons engaged in investment activities in Iran created by DGS; or b) demonstrate it has been exempted from the certification requirement for that solicitation or contract pursuant to Public Contract Code § 2203(c) or (d).

To comply with this requirement, please insert your vendor or financial institution name and Federal ID Number (if available) and complete one of the options below. Please note: California law establishes penalties for providing false certifications, including civil penalties equal to the greater of \$250,000 or twice the amount of the contract for which the false certification was made; contract termination; and three-year ineligibility to bid on contracts. (Public Contract Code § 2205.)

OPTION #1 - CERTIFICATION

I, the official named below, certify I am duly authorized to execute this certification on behalf of the vendor/financial institution identified below, and the vendor/financial institution identified below is not on the current list of persons engaged in investment activities in Iran created by DGS and is not a financial institution extending twenty million dollars (\$20,000,000) or more in credit to another person/vendor, for 45 days or more, if that other person/vendor will use the credit to provide goods or services in the energy sector in Iran and is identified on the current list of persons engaged in investment activities in Iran created by DGS.

Vendor Name/Financial Institution (Printed):	Federal ID Number (or n/a):
By (Authorized Signature):	
Printed Name and Title of Person Signing:	
Date Executed:	Executed in

OPTION #2 – EXEMPTION

Pursuant to Public Contract Code sections 2203(c) and (d), a public entity may permit a vendor/financial institution engaged in investment activities in Iran, on a case-by-case basis, to be

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

eligible for, or to bid on, submit a proposal for, or enters into or renews, a contract for goods and services.

If you have obtained an exemption from the certification requirement under the Iran Contracting Act, please fill out the information below, and attach documentation demonstrating the exemption approval.

Vendor Name/Financial Institution (Printed):	Federal ID Number (or n/a)
By (Authorized Signature)	
Printed Name and Title of Person Signing:	Date Executed:

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015

EXHIBIT 11: SURETY AND OTHER SECURITY DOCUMENTS (Not Applicable)

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

EXHIBT 12: DVBE DECLARATIONS

A copy of the STD. 843, Disabled Veteran Business Enterprise Declarations and its instructions is available as a fill and print PDF at:

<http://www.documents.dgs.ca.gov/pd/poliproc/STD-843FillPrintFields.pdf>

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

EXHIBIT 13: BIDDING PREFERENCES AND INCENTIVES**ALL BIDDERS: COMPLETE ALL SECTIONS BELOW AND SUBMIT WITH YOUR PROPOSAL.****1. SMALL BUSINESS PREFERENCE:**

Bidder must check the appropriate box from the choices below.

- I am a DGS certified Small Business and claim the Small Business Preference.
My DGS Small Business certification number is: _____
- I have recently filed for DGS Small Business preference but have not yet received certification, but I am claiming the Small Business preference.
- I am not a DGS certified Small Business, but 25% or more of the revenue from the award will go to DGS certified Small Business Subcontractors performing a Commercially Useful Function and therefore I am claiming the preference.

Bidder must complete and submit Exhibit 5: GSPD-05-105 Bidder Declaration, indicating the percentage of the revenue that will be received by each DGS certified Small Business Subcontractor. The form can also be found at the following link:

<http://www.documents.dgs.ca.gov/pd/poliproc/Master-Biddeclar08-09.pdf>

- I am not claiming the DGS Small Business preference.

2. DVBE INCENTIVE:

Bidder must check the appropriate box from the choices below.

- I am a DGS certified DVBE. A copy of my STD. 843 form is attached.
- I have recently filed for DGS DVBE certification, but have not yet received certification.
- I am not a DGS certified DVBE, but a percentage of the revenue will be going to DGS certified DVBE Subcontractors performing a Commercially Useful Function, and therefore I am claiming the DVBE incentive.

Bidder must submit a complete Exhibit 5: GSPD-05-105, Bidder Declaration, indicating the percentage of the revenue that will be received by each DGS certified DVBE Subcontractor. Bidder must also submit an Exhibit 12, STD 843 DVBE Declarations, for each DVBE Subcontractor, signed by the DVBE owner/manager. The form can be found on the following link:

<http://www.documents.dgs.ca.gov/pd/poliproc/STD-843FillPrintFields.pdf>

- I am not claiming the DVBE incentive.

3. ADDITIONAL BIDDING PREFERENCES:

The Bidder shall check the appropriate box or boxes from the choices below.

I am not claiming the TACPA preference.

I am claiming the TACPA bidding preference.

Bidder must submit Exhibit 15: STD 830 TACPA Preference Request.

Name of Bidder:

Signature and Date:

EXHIBIT 14: COMMERCIALLY USEFUL FUNCTION (CUF) CERTIFICATION**Bidder Name:** _____**COMMERCIALLY USEFUL FUNCTION DOCUMENTATION**

All certified small business, micro business, and/or DVBE Contractors, subcontractors or suppliers must meet the commercially useful function requirements under Government Code Section 14837 (for SB) and Military and Veterans Code Section 999(e)(2)(for DVBE).

Please answer the following questions, as they apply to your company for the goods and services being acquired in this solicitation.

Subcontractor Name (submit one form for each SB/DVBE): _____

Mark all that apply: DVBE: Small Business: Micro Business: N/A:

1.	Will the subcontractor be responsible for the execution of a distinct element of the resulting Contract?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2.	Will this subcontractor be actually performing, managing, or supervising an element of the resulting Contract?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
3.	Will this subcontractor be performing work on the resulting Contract that is normal for its business, services, and functions?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4.	Will there be any further subcontracting that is greater than that expected to be subcontracted by normal industry practices for the resulting Contract?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
5.	Will this subcontractor be responsible, with respect to products, inventories, materials, and supplies required for the contract, for negotiating price, determining quality and quantity, ordering, installing, if applicable, and making payment?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

A response of "No" in questions 1-3 or a response of "Yes" in question 4, may result in your proposal being deemed non-responsive and disqualified.

The bidder must provide a written statement below detailing the role, services and goods the subcontractor(s) will provide to meet the commercially useful function requirement. If the bidder is not claiming a Small Business or DVBE, indicate "Not claiming a preference" in the box below.

At the State's option prior to award, bidders may be required to submit additional written clarifying information.

By signing this form, the undersigned bidder certifies that the Certified Small Business or DVBE satisfies the Commercially Useful Function requirement, and will provide the role, services, and/or goods stated above.

Contractor Signature: _____

Contractor Printed/Typed Name and Title: _____

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

EXHIBIT 15: STD 830 TACPA PREFERENCE REQUEST

A copy of the *STD 830 TACPA Preference Request* and its instructions is available as a fill and print PDF at: <http://www.documents.dgs.ca.gov/dgs/fmc/pdf/std830.pdf>

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

EXHIBIT 16: LIST OF PROPOSED SUBCONTRACTORS (PUBLIC WORKS) *(NOT APPLICABLE)

Listed hereinafter is the name and address of each subcontractor who will be employed and the kind of work which each will perform if the contract is awarded to the aforesigned. I understand that under Government Code Section 4100 through 4113* (See Note Below) I must here clearly set forth the name and address of each subcontractor who will perform work or labor or render service to me in or about the construction of the work in an amount in excess of one-half of one percent (1/2 of 1%) of my total proposal and that as to any work in which I fail to do so, I agree to perform that portion myself or be subject to penalty under the act.

(NOTE: IF MORE THAN ONE SUBCONTRACTOR IS LISTED FOR THE SAME TYPE OF WORK, STATE THE PORTION OF THAT TYPE OF WORK THAT THE INDIVIDUAL SUBCONTRACTOR WILL BE PERFORMING. LIST THE SUBCONTRACTORS' APPLICABLE CONTRACTORS LICENSE NUMBER(S), IF AVAILABLE. VENDORS OR SUPPLIERS OF MATERIALS ONLY, NEED NOT BE LISTED.)

If additional space is required for the listing of proposed subcontractors, reproduced additional sheets showing the required information, as indicated below, shall be attached hereto and made a part of the Final Bid proposal.

SUBCONTRACTOR NAME AND ADDRESS	TYPE OF WORK	LICENSE NO.	EXPIRATION DATE

NOTE: The above listing requirement will for purposes of this proposal be construed in accordance with the provisions of the Subletting and Subcontracting Fair Practices Act ("The Act") as set forth in Government Code Sections 4100 through 4113. Also, for purposes of this proposal and interpretation of The Act, a vendor will be considered to be a prime contractor regardless of whether such vendor is or is not a licensed contractor.

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

EXHIBIT 17: CONTRACTOR’S LICENSE INFORMATION *(NOT APPLICABLE)

(Installation Services Only)

Bidder shall complete the applicable contractor’s license information below in accordance with the Contractor’s State License Board, Department of Consumer Affairs. A Contractor’s license of appropriate Class **{Agency conducting the bid must specify the Class of license required for the specific solicitation}** is required before any Bidder can contract business (e.g. submit a proposal) which includes the installation of cable and wiring, electrical modification. In addition, if structural modifications are required, a Class B license is required.

CONTRACTOR:

Class _____ License No: _____

Licensee: _____ Expiration Date: _____

Note: Bidder (Firm’s Name or a Responsible Managing Employee) must be licensed in addition to all subcontractor(s) performing under this contract.

SUBCONTRACTOR 1:

Class _____ License No: _____

Licensee: _____ Expiration Date: _____

Relationship of Licensee to Contractor:_____

SUBCONTRACTOR 2:

Class _____ License No: _____

Licensee: _____ Expiration Date: _____

Relationship of Licensee to Contractor:_____

(Use additional sheets if necessary.)

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

EXHIBIT 18: BIDDER QUALIFICATION FORM - INSTRUCTIONS

The Bidder must complete the project information required that qualifies for the duties and responsibilities for the experience.

Exhibits 18.1 and 18.2 will be used by Office of Systems Integration (OSI) to evaluate Bidder’s qualifications. The Bidder must specify the required experience in the pertinent row of Exhibit 18.1. Use additional forms as needed to complete each question. OSI may contact references listed on Exhibit 18.2 to verify the information provided by the Bidder. Any conflicting information may result in the bid being deemed non-responsive and may result in the bid being disqualified.

The Bidder must complete the Bidder Qualification Form Exhibit 18.1 in accordance with the instructions provided below. One Attachment must be completed for each separate project used to meet the minimum Mandatory experience requirements.

All dates must be in MM/DD/YYYY format.

Bidder’s references cannot be any individual involved in the development of this RFP or the solicitation process for this contract. Bidder’s references may be contacted to verify information provided by the Bidder.

Box 1, Bidder Name: Provide the name of the company submitting the proposal.

Box 2, Project Name and Description: Provide the project name and give a brief description of the nature of the project.

Boxes 3, Company name of the Bidder’s Reference.

Box 4, Contact name and contact information of the Bidder’s reference.

Boxes 5 and 6, Start Date and End Date: Provide the start and end date the bidder worked on the cited project using MM/DD/YYYY format.

Boxes 7, Check the appropriate response, “Yes” or “No”.

Boxes 8, Check the appropriate response, “Yes” or “No”.

Box 9, Project Contract Amount: Provide the dollar amount of the Project Contract.

Box 10, Instructions for documenting the years of experience gained from the project cited.

Note: It is the Bidder’s responsibility to ensure that each Minimum Experience Requirement is met in full and addressed in the Bidder Qualification Forms so that the State can establish compliance. If the State cannot determine that the years of experience for each of the Minimum Experience Requirements has been met, your bid may be deemed non-responsive.

EXHIBIT 18.1: BIDDER QUALIFICATIONS FORM

Bidders may use multiple projects to meet the total experience required for each Mandatory Experience and, if applicable, Desirable Experience. A separate form must be completed for each project cited.

1	Bidder Name:			
2	Project Name and Description:			
3	Company Name of Bidder’s Reference:			
4	Contact Name, email Address and Telephone Number of Bidder’s reference:			
5	Start Date (MM/DD/YYYY):			
6	End Date (MM/DD/YYYY):			
7	Was the Bidder that Performed the Work the Prime Contractor? Yes ___ No ___			
8	Did the Bidder Complete the Project? Yes ___ No ___ On-going (see line #6 for contract completion date)			
9	Project Contract Amount: \$			
10	For each Mandatory Experience below, check “yes” if the Total Experience Requirement was met on this cited Project; check “no” if none of the experience was met on this cited Project; or check “Partial” if some of the experience was met on this cited Project. If partial or total experience was met, enter the years and/or months of “Experience gained on this cited Project” and the Bidder’s duties and responsibilities performed on the Project in the “Bidder’s Description of Services Provided” field.			
Number	Classification	Mandatory Experience	Experience Required	Experience gained on this cited Project
1	M	Legacy Replacement The Bidder must have replaced a legacy IT system that has been accepted by the client and is in Production as of the Final Proposal submission date for this RFP. The Bidder must have successfully converted the data from more than one relational database and migrated it to the replacement system.	2 Years	Yes ___ No ___ Partial ___ Yr. ___ Mo ___

<i>Bidder's Description of Services Provided:</i>				
2	M	<p>Application Program Interface</p> <p>The Bidder must have demonstrated experience developing secure RESTful Web Application Program Interfaces (APIs). These APIs must demonstrate simplifying component implementation, reduce the complexity of connector semantics, improve the effectiveness of performance tuning, and increase the scalability of pure server components.</p>	2 Years	Yes _____ No _____ Partial _____ Yr. ___ Mo ___
<i>Bidder's Description of Services Provided:</i>				
3	M	<p>Application Integration</p> <p>The Bidder must have successfully integrated dissimilar systems with file-based and service-based interfaces. The Bidder must have demonstrated the capability to use adapters to bind to legacy assets, perform protocol mediation (e.g., transform a proprietary protocol into a standardized application processing interface), and throttle middleware infrastructure to meet performance requirements.</p>	2 Years	Yes _____ No _____ Partial _____ Yr. ___ Mo ___
<i>Bidder's Description of Services Provided:</i>				
4	M	<p>Agile Development</p> <p>The Bidder must demonstrated experience in scrum-based agile processes in sprint execution activities (e.g., user story development, product backlog maintenance, user story user-acceptance, retrospective, and product review).</p>	2 Years	Yes _____ No _____ Partial _____ Yr. ___ Mo ___
<i>Bidder's Description of Services Provided:</i>				

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

5	M	<p>Source Code Management</p> <p>The Bidder must demonstrate documentation within the code itself (e.g., through proper use of descriptive commit messages, issue tracking, pull requests, etc.), and the management all assets (e.g., source code, automated tests, user stories, configuration files, knowledge transfer material, etc.).</p>	2 Years	Yes _____ No _____ Partial _____ Yr. ___ Mo ___
<i>Bidder's Description of Services Provided:</i>				

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

EXHIBIT 18.2: BIDDER REFERENCE FORM

Bidder Instructions: Complete the first six (6) fields of this Exhibit 18.2, Bidder Reference Form, for each corresponding Exhibit 18.1, Bidder Qualification Forms submitted. The Bidder’s reference must complete the rest of this form. The reference information below must be the same as the corresponding Exhibit 18.1. Include a copy of the corresponding Exhibit 18.1 with Exhibit 18.2, Bidder Reference Form to Bidder’s References for completion.

Instructions for the Bidder’s References: Using the rating scale in the “Reference Satisfaction Rating” field, please rate your satisfaction with the Bidder who performed the services described on Exhibit 18.1. Date and sign this Exhibit 18.2 and return the form(s) to the Bidder.

1	Bidder Name:	
2	Project Name:	
3	Company Name of Bidder’s Reference:	
4	Contact Name, Email Address, and Telephone Number of Bidder’s Reference:	
5	Bidder’s involvement:	
6	Project Description:	
<u>Reference Satisfaction Rating</u> Using the following scale: 0 = Unsatisfactory, 2 = Marginal, 3 = Satisfactory, 4 = Exceeds Expectations, 6 = Excellent Please rate your satisfaction with the staff that provided the services described in Exhibit 18.1. Circle only one number for each question below.		
7	How would you rate the Bidder’s effectiveness at delivering software solutions using an agile methodology?	0 2 3 4 6
8	How would you rate the quality and professionalism of the Bidder’s staff?	0 2 3 4 6
9	How would you rate the Contractor’s overall performance?	0 2 3 4 6
Total Possible Points (9)		

By signing below, I declare that I have reviewed the information contained in Exhibit 18.1 and that the information is true and correct.

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

Reference Signature:

Date:

Printed Name:

Reference Project Role:

Reference Email

Reference

Phone:

EXHIBIT 19: STAFF QUALIFICATIONS FORM INSTRUCTIONS

The Bidder must complete the project information required below that qualifies the Bidder’s team members for the duties and responsibilities for the mandatory roles.

The Bidder must complete the Staff Qualification Forms for each staff in accordance with the instructions provided below. A Separate Exhibit must be completed for each separate project used to meet the minimum mandatory requirements.

All dates must be in MM/DD/YYYY format.

Bidder’s references **cannot be any individual involved in the development of this RFP or the solicitation process for this contract.**

Box 1, Bidder Name: Provide the name of the company submitting the bid proposal.

Box 2, Staff Name: Provide the name of the proposed staff.

Box 3, Project Name and Description: Provide the project name and give a brief description of the nature of the project.

Box 4, Company Name of Staff’s Reference:

Box 5, Contact Information of Staff’s Reference: Provide the company name of staff’s reference, contact person and their email address and phone number.

Boxes 6 and 7, Staff Start Date and End Date: Provide the start and end date the staff person worked on the cited project using MM/DD/YYYY format.

Box 8, Instructions for documenting the years of experience gained from the project cited.

Note: It is the Bidder’s responsibility to ensure that each Minimum Experience Requirement is met in full and addressed in the Staff Qualification Forms so that the State can establish compliance. If the State cannot determine that the years of experience for each of the Minimum Experience Requirements has been met, your bid may be deemed non-response.

EXHIBIT 19.1: MANAGEMENT LEAD/ACCOUNT REPRESENTATIVE QUALIFICATIONS FORM

Bidders may use multiple projects to meet the Total Experience Required for each Mandatory Experience and, if applicable, Desirable Experience. A separate form must be completed for each project cited.

1	Bidder Name:			
2	Staff Name:			
3	Staff’s referenced Project Name and Description:			
4	Company Name of Staff’s reference:			
5	Contact Name, email Address and Telephone Number of staff’s reference:			
6	Staff Start Date (MM/DD/YYYY):			
7	Staff End Date (MM/DD/YYYY):			
8	For each Mandatory Experience below, check “yes” if the Total Experience Requirement was met on this cited Project; check “no” if none of the experience was met on this cited Project; or check “Partial” if some of the experience was met on this cited Project. If partial or total experience was met, enter the years and/or months of “Experience gained on this cited Project” and the Staff’s duties and responsibilities performed on the Project in the “Bidder’s Description of Services Provided” field.			
Number	Classification	Mandatory Qualifications	Experience Required	Experience gained on this cited Project
9	M	The Management Lead shall have been responsible for the management of a system similar in scope to the Bidder’s proposed solution.	2 Years	Yes ____ No ____ Partial ____ Yr. ____ Mo ____
	<i>Bidder’s Description of Services Provided:</i>			
10	M	The Management Lead shall have been involved in and led a minimum of two software development projects similar in scope to the Bidder’s proposed solution.	2 Years	Yes ____ No ____ Partial ____ Yr. ____ Mo ____
	<i>Bidder’s Description of Services Provided:</i>			

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

Number	Classification	Mandatory Qualifications	Experience Required	Experience Gained on This Cited Project
11	M	<p>The Management Lead shall have a baccalaureate degree from an accredited college or university in a related field, or commensurate experience.</p> <p>Attach a copy of degree certificate or other proof of education requirement.</p>	or 6 Years	<p>Yes <input type="checkbox"/></p> <p>No <input type="checkbox"/></p> <p>Partial <input type="checkbox"/></p> <p>Yr. <input type="text"/> Mo <input type="text"/></p>
<i>Bidder's Description of Services Provided</i>				

EXHIBIT 19.2 MANAGEMENT LEAD/ACCOUNT REPRESENTATIVE - REFERENCE FORM

Bidder Instructions: Complete the first four (4) fields of this Exhibit 19.2, Staff Reference Form, for each corresponding Exhibit 19.1. The reference information below must correspond to Exhibit 19.1. The Bidder’s reference must complete the rest of this form. Include Exhibit 19.2 with the corresponding Exhibit 19.1 to Staff’s reference for completion.

Staff’s Reference Instructions: Using the rating scale in the “Reference Satisfaction Rating” field, please rate your satisfaction with the Staff who performed the services described on Exhibit 19.1. This Exhibit must be completed in its entirety, signed and dated by a client reference contact that performed a technical or supervisory role on the referenced project to be considered responsive. Date and sign this Exhibit 19.2 and return the forms to the Bidder.

1	Bidder’s Staff Name:	
2	Project Name:	
3	Company Name of Staff’s Reference:	
4	Contact Name, Email Address, and Telephone Number of Staff’s Reference:	
	<u>Reference Satisfaction Rating</u> Using the following scale: 0 = Unsatisfactory, 2 = Marginal, 3 = Satisfactory, 4 = Exceeds Expectations, 6 = Excellent Please rate your satisfaction with the staff that provided the services described in Exhibit 19.1 Circle only one number for each question below.	
5	Rate the quality and timeliness of the work products for which this individual was responsible.	0 2 3 4 6
6	Rate the individual’s interpersonal, oral, written communication and collaboration skills.	0 2 3 4 6
7	Rate the individual’s knowledge in the required areas of expertise for this engagement.	0 2 3 4 6
Total Possible Points (18)		

By signing below, I declare that I have reviewed the information contained in Exhibit 19.1 and that the information is true and correct.

Reference Signature:

Date:

Printed Name:

Reference Project Role:

Reference Email

Reference Phone:

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015

EXHIBIT 19.3: LEAD DEVELOPER QUALIFICATIONS FORM

Bidders may use multiple projects to meet the Total Experience Required for each Mandatory Experience and, if applicable, Desirable Experience. A separate form must be completed for each project cited.

1	Bidder Name:			
2	Staff Name:			
3	Staff’s referenced Project Name and Description:			
4	Company Name of Staff’s reference:			
5	Contact Name, email Address and Telephone Number of staff’s reference:			
6	Staff Start Date (MM/DD/YYYY):			
7	Staff End Date (MM/DD/YYYY):			
8	For each Mandatory Experience below, check “yes” if the Total Experience Requirement was met on this cited Project; check “no” if none of the experience was met on this cited Project; or check “Partial” if some of the experience was met on this cited Project. If partial or total experience was met, enter the years and/or months of “Experience gained on this cited Project” and the Staff’s duties and responsibilities performed on the Project in the “Bidder’s Description of Services Provided” field.			
Number	Classification	Mandatory Qualifications	Experience Required	Experience gained on this cited Project
9	M	The Lead Developer shall have been responsible for the development of a system similar in scope to the Bidder’s proposed solution.	3 Years	Yes _____ No _____ Partial _____ Yr. ___ Mo ___
	<i>Bidder’s Description of Services Provided:</i>			
10	M	The Lead Developer shall have been involved in and led a minimum of two software development projects similar in scope to the Bidder’s proposed solution.	3 Years	Yes _____ No _____ Partial _____ Yr. ___ Mo ___
	<i>Bidder’s Description of Services Provided:</i>			

Number	Classification	Mandatory Qualifications	Experience Required	Experience Gained on This Cited Project
11	M	The Lead Developer shall have a minimum of three (3) years of management experience with software development, design, and the System Development Life Cycle (SDLC) methodologies proposed by the Bidder.	3 Years	Yes ____ No ____ Partial ____ Yr. __ Mo __
<i>Bidder's Description of Services Provided</i>				
12	M	The Lead Developer shall have a computer science, engineering, or technology-related baccalaureate degree from an accredited college or university, or commensurate experience. Attach a copy of degree certificate or other proof of education requirement.	Or 7 Years	Yes ____ No ____ Partial ____ Yr. __ Mo __
<i>Bidder's Description of Services Provided:</i>				

EXHIBIT 19.4: LEAD DEVELOPER - REFERENCE FORM

Bidder Instructions: Complete the first four (4) fields of this Exhibit 19.4, Staff Reference Form, for each corresponding Exhibit 19.3. The reference information below must correspond to Exhibit 19.3. The Bidder’s reference must complete the rest of this form. Include Exhibit 19.4 with the corresponding Exhibit 19.3 to Staff’s reference for completion.

Staff’s Reference Instructions: Using the rating scale in the “Reference Satisfaction Rating” field, please rate your satisfaction with the Staff who performed the services described on Exhibit 19.3. This Exhibit must be completed in its entirety, signed and dated by a client reference contact that performed a technical or supervisory role on the referenced project to be considered responsive. Date and sign this Exhibit 19.4 and return the forms to the Bidder.

1	Bidder’s Staff Name:	
2	Project Name:	
3	Company Name of Staff’s Reference:	
4	Contact Name, Email Address, and Telephone Number of Staff’s Reference:	
<u>Reference Satisfaction Rating</u> Using the following scale: 0 = Unsatisfactory, 2 = Marginal, 3 = Satisfactory, 4 = Exceeds Expectations, 6 = Excellent Please rate your satisfaction with the staff that provided the services described in Exhibit 19.3 Circle only one number for each question below.		
5	Rate the quality and timeliness of the work products for which this individual was responsible.	0 2 3 4 6
6	Rate the individual’s interpersonal, oral, written communication and collaboration skills.	0 2 3 4 6
7	Rate the individual’s knowledge in the required areas of expertise for this engagement.	0 2 3 4 6
Total Possible Points (18)		

By signing below, I declare that I have reviewed the information contained in Exhibit 19.4 and that the information is true and correct.

Reference Signature:

Date:

Printed Name:

Reference Project Role:

Reference Email

Reference Phone:

**State of California
Office of Systems Integration**

**RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015**

EXHIBIT 19.5: SCRUM MASTER QUALIFICATIONS FORM

Bidders may use multiple projects to meet the Total Experience Required for each Mandatory Experience and, if applicable, Desirable Experience. A separate form must be completed for each project cited.

1	Bidder Name:			
2	Staff Name:			
3	Staff’s referenced Project Name and Description:			
4	Company Name of Staff’s reference:			
5	Contact Name, email Address and Telephone Number of staff’s reference:			
6	Staff Start Date (MM/DD/YYYY):			
7	Staff End Date (MM/DD/YYYY):			
8	For each Mandatory Experience below, check “yes” if the Total Experience Requirement was met on this cited Project; check “no” if none of the experience was met on this cited Project; or check “Partial” if some of the experience was met on this cited Project. If partial or total experience was met, enter the years and/or months of “Experience gained on this cited Project” and the Staff’s duties and responsibilities performed on the Project in the “Bidder’s Description of Services Provided” field.			
Number	Classification	Mandatory Qualifications	Experience Required	Experience gained on this cited Project
9	M	The Scrum Master shall have been responsible for the management of a system similar in scope to the Bidder’s proposed solution.	2 Years	Yes _____ No _____ Partial _____ Yr. ___ Mo ___
<i>Bidder’s Description of Services Provided:</i>				
10	M	The Scrum Master shall have been involved in and led a minimum of two software development projects similar in scope to the Bidder’s proposed solution.	2 Years	Yes _____ No _____ Partial _____ Yr. ___ Mo ___
<i>Bidder’s Description of Services Provided:</i>				

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

Number	Classification	Mandatory Qualifications	Experience Required	Experience Gained on This Cited Project
11	M	<p>The Scrum Master shall hold a certification related to Scrum.</p> <p>*Attach copy of certification</p>		
<i>Bidder's Description of Services Provided</i>				
12	M	<p>The Scrum Master shall have a baccalaureate degree from an accredited college or university in a related field, or commensurate experience. Attach a copy of degree certificate or other proof of education requirement.</p>	<i>Or 6 Years</i>	Yes <input type="checkbox"/> No <input type="checkbox"/> Partial <input type="checkbox"/> Yr. <input type="text"/> Mo <input type="text"/>
<i>Bidder's Description of Services Provided:</i>				

EXHIBIT 19.6: SCRUM MASTER - REFERENCE FORM

Bidder Instructions: Complete the first four (4) fields of this Exhibit 19.6, Staff Reference Form, for each corresponding Exhibit 19.5. The reference information below must correspond to Exhibit 19.5. The Bidder’s reference must complete the rest of this form. Include Exhibit 19.6 with the corresponding Exhibit 19.5 to Staff’s reference for completion.

Staff’s Reference Instructions: Using the rating scale in the “Reference Satisfaction Rating” field, please rate your satisfaction with the Staff who performed the services described on Exhibit 19.5. This Exhibit must be completed in its entirety, signed and dated by a client reference contact that performed a technical or supervisory role on the referenced project to be considered responsive. Date and sign this Exhibit 19.6 and return the forms to the Bidder.

1	Bidder’s Staff Name:	
2	Project Name:	
3	Company Name of Staff’s Reference:	
4	Contact Name, Email Address, and Telephone Number of Staff’s Reference:	
	<u>Reference Satisfaction Rating</u> Using the following scale: 0 = Unsatisfactory, 2 = Marginal, 3 = Satisfactory, 4 = Exceeds Expectations, 6 = Excellent Please rate your satisfaction with the staff that provided the services described in Exhibit 19.5 Circle only one number for each question below.	
5	Rate the quality and timeliness of the work products for which this individual was responsible.	0 2 3 4 6
6	Rate the individual’s interpersonal, oral, written communication and collaboration skills.	0 2 3 4 6
7	Rate the individual’s knowledge in the required areas of expertise for this engagement.	0 2 3 4 6
Total Possible Points (18)		

By signing below, I declare that I have reviewed the information contained in Exhibit 19.5 and that the information is true and correct.

Reference Signature:

Date:

Printed Name:

Reference Project Role:

Reference Email

Reference Phone:

EXHIBIT 19.7: PRODUCT DEVELOPMENT TEAM QUALIFICATIONS FORM

Bidders may use multiple projects to meet the Total Experience Required for each Mandatory Experience and, if applicable, Desirable Experience. A separate form must be completed for each project cited.

1	Bidder Name:			
2	Staff Name:			
3	Staff’s referenced Project Name and Description:			
4	Company Name of Staff’s reference:			
5	Contact Name, email Address and Telephone Number of staff’s reference:			
6	Staff Start Date (MM/DD/YYYY):			
7	Staff End Date (MM/DD/YYYY):			
8	For each Mandatory Experience below, check “yes” if the Total Experience Requirement was met on this cited Project; check “no” if none of the experience was met on this cited Project; or check “Partial” if some of the experience was met on this cited Project. If partial or total experience was met, enter the years and/or months of “Experience gained on this cited Project” and the Staff’s duties and responsibilities performed on the Project in the “Bidder’s Description of Services Provided” field.			
Number	Classification	Mandatory Qualifications	Experience Required	Experience gained on this cited Project
9	M	Each member of the Product Development Team shall have been involved in at least two software development projects similar in scope to the Bidder’s proposed solution.	2 Years	Yes _____ No _____ Partial _____ Yr. ___ Mo ___
	<i>Bidder’s Description of Services Provided:</i>			
10	M	Each member of the Product Development Team shall have been involved in at least one agile software development project.	2 Years	Yes _____ No _____ Partial _____ Yr. ___ Mo ___

<i>Bidder's Description of Services Provided:</i>				
Number	Classification	Mandatory Qualifications	Experience Required	Experience Gained on This Cited Project
12	M	<p>1. Each member of the Product Development Team shall have at least 2 years experience in at least one of the following, and between all team members each of the following must be covered. Attach a separate matrix mapping the staff to the qualifications.</p> <ul style="list-style-type: none"> a. COBOL and Assembly in a CICS mainframe environment b. CICS COBOL API in a SQL DB environment c. VB6 d. Secure REST APIs e. Enterprise user authentication tools f. Modern security, monitoring, and logging practices for system administration g. Modular web application development h. Test-driven development i. Automated unit and integration testing j. Automated acceptance testing k. Continuous build processes and tools l. SQL and SQL optimization m. Load and Performance testing n. Security and system administration o. Modern continuous monitoring tools <p>NIST 800-53 controls</p>	2 Years	Yes _____ No _____ Partial _____ Yr. ___ Mo ___
<i>Bidder's Description of Services Provided:</i>				

EXHIBIT 19.8: PRODUCT DEVELOPMENT TEAM - REFERENCE FORM

Bidder Instructions: Complete the first four (4) fields of this Exhibit 19., Staff Reference Form, for each corresponding Exhibit 19.7. The reference information below must correspond to Exhibit 19.7. The Bidder’s reference must complete the rest of this form. Include Exhibit 19.8 with the corresponding Exhibit 19.7 to Staff’s reference for completion.

Staff’s Reference Instructions: Using the rating scale in the “Reference Satisfaction Rating” field, please rate your satisfaction with the Staff who performed the services described on Exhibit 19.7. This Exhibit must be completed in its entirety, signed and dated by a client reference contact that performed a technical or supervisory role on the referenced project to be considered responsive. Date and sign this Exhibit 19.8 and return the forms to the Bidder.

1	Bidder’s Staff Name:	
2	Project Name:	
3	Company Name of Staff’s Reference:	
4	Contact Name, Email Address, and Telephone Number of Staff’s Reference:	
<u>Reference Satisfaction Rating</u> Using the following scale: 0 = Unsatisfactory, 2 = Marginal, 3 = Satisfactory, 4 = Exceeds Expectations, 6 = Excellent Please rate your satisfaction with the staff that provided the services described in Exhibit 19.7 Circle only one number for each question below.		
5	How would you rate the individual’s overall performance?	0 2 3 4 6
6	How would you rate the individual’s effectiveness at communicating (orally and in writing) with project members and stakeholders?	0 2 3 4 6
7	How would you rate the individual’s effectiveness at dealing with project conflicts and conflicting priorities?	0 2 3 4 6
Total Possible Points (18)		

By signing below, I declare that I have reviewed the information contained in Exhibit 19.7 and that the information is true and correct.

Reference Signature:

Date:

Printed Name:

Reference Project Role:

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015

Reference Email

Reference Phone:

PAGE INTENTIONALLY LEFT BLANK

EXHIBIT 20: REQUIREMENTS CERTIFICATION (M)
(FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS CONTAINED IN THE STATEMENT OF WORK)

By signing this document, the Bidder agrees to:

- Comply with all RFP #31326 Mandatory requirements (Section 5 SOW).

Failure to sign this certification may result in the proposal being deemed nonresponsive.

Signature of Bidder Representative with legal authorization to bind the firm:	
Typed Name and Title of Bidder Representative:	
Bidder Name:	
Street Address:	
City, State, Zip	
Phone Number, including area code:	
E-mail Address:	
Date Signed:	

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

EXHIBIT 21: PROPOSAL NARRATIVE REQUIREMENTS (MS)

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

EXHIBIT 22: COST WORKSHEETS

Refer to the Excel Workbook file on Cal eProcure labeled, “Exhibit 22 Cost Worksheets” for submission of your Cost Information.

The cost table format the bidder must submit with their Final Proposals is included in the separate Excel Workbook, *Exhibit 22 Cost Worksheets*. The Cost Worksheets in this workbook shall be filled out by the Bidder in accordance with the instructions in Section 6, *PROPOSAL AND BID FORMAT* and in the these Cost Worksheets shall be submitted with the Bidders Final Bid as Volume 3, in a separately sealed envelope.

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

EXHIBIT 23: BIDDERS' LIBRARY ACCESS AUTHORIZATION FORM

The following information, along with a completed Exhibit 3 Confidentiality Statement, must be provided in order to receive authorization to access the CWS-NS Bidders' Library. For information on accessing the Bidders' Library, refer to the CWS-NS Bidders' Library Access and User's Guide.

The Bidders' Library allows bidders access to documents and information to help bidders understand CWS-NS requirements and prepare a proposal response. Material includes, but is not limited to, CWS-NS laws and regulations; policies, manuals and guides, business and technical data, and information on current systems and processes. All RFP OSI #31326 CWS-NS requirements, terms, conditions, rules, and instructions are included or referenced in the solicitation. Bidders are not required to use the supplemental information, but are strongly encouraged to do so. Bidders are advised to check for periodic updates. The State does not guarantee the accuracy or the relevancy of the supplemental information and any of the supplemental information relied upon is at the Bidder's risk.

The individual to whom the Bidders' Library access information should be transmitted is:

Name	Title		
<hr/>			
Company			
Street Address	City	State	Zip
() -	() -		
Phone (xxx) xxx-xxxx	Fax (xxx) xxx-xxxx		
<hr/>			
E-mail Address			

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 1 – TEMPLATE FOR QUESTION SUBMITTAL

(This Attachment provides the format for which a bidder shall submit questions regarding this solicitation and is not required to be submitted with your proposal response.)

Bidders are requested to use this form when submitting questions to the Procurement Official listed in Section 1.6. Instructions are as follows:

Name of Bidder – Provide the name of the Bidding firm

Contact Person – Provide the name of the person to contact if the State needs clarification about the question.

Contact Email and Phone # – Provide the email and phone number (including area code) for the listed contact person.

Q # – Sequentially number each question, always starting at one (1) for each submission.

Document(s) – Identify the section or document(s) the question pertains to.

Page/Section # – Identify the page and section number(s) that the question pertains to.

Question – Write the question in this column.

Expand or reduce the number of rows to accommodate the number of questions.

Table-1 Question Submittal Form

SOLICITATION Bidder Question Form			
Name of Bidder:			
Contact Person:			
Contact Email and Phone Number:			
Q #	Document(s)	Page/Section #	Question
1			
2			
3			

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder’s Response
December 21, 2015

4			
---	--	--	--

PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 2 – TEMPLATE FOR REQUEST FOR CHANGES SUBMITTAL

(This Attachment provides the format for which a bidder shall submit requests for changes to this solicitation and is not required to be submitted with your solicitation response).

Bidders are requested to use this form when submitting request for changes to the Procurement Official listed in Section 2.2.1. Instructions are as follows:

Name of Bidder – Provide the name of the Bidding firm

Contact Person – Provide the name of the person to contact if the State needs clarification about the request for change.

Contact Email and Phone # – Provide the email and phone number (including area code) for the listed contact person.

Ch # – Sequentially number each change, always starting at one (1) for each submission.

Document(s) – Identify the document(s) the request pertains to, such as “Section 3, Administrative Requirements”.

Page/Section # – Identify the page and section number(s) that the change pertains to.

Proposed Change – Write the requested change in this column. The Bidder shall apply tracked changes to ensure the change is evident.

Expand or reduce the number of rows to accommodate the number of questions.

Table-2 Bidder Request for Change Form

RFP Bidder Request for Change Form				
Name of Bidder:				
Contact Person:				
Contact Email and Phone Number:				
Ch #	Document(s)	Page/Section #	Proposed Change (redlined)	Bidder’s Rationale
1				
2				
3				

State of California
Office of Systems Integration

RFP OSI 31326
Part 2 – Bidder's Response
December 21, 2015

PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 3: PROCEDURES FOR CONDUCTING PROTESTS UNDER THE ALTERNATIVE PROTEST PROCESS

(This Attachment is not required to be submitted with your solicitation response.)

California Code of Regulations, Title 1, Division 2.**Chapter 5. Procedures for Conducting Protests under the Alternative Protest Process****Article 1. General Provisions****§1400. Purpose; Scope of Chapter.**

Protests under the Alternative Protest Pilot Project (AB 1159, Chapter 762 of 1997 Statutes, Public Contract Code Division 2, Part 2, Chapter 3.6 (sections 12125-12130)) shall be resolved by arbitration as defined and established by this chapter.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New chapter 5 (articles 1-3), article 1 (sections 1400-1404) and section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1402. Definitions.

- (a) Arbitration, as used in this chapter, means a dispute resolution procedure in which the Department of General Services, Office of Administrative Hearings provides a neutral third party who decides the merits of a protest and issues a binding decision to the Parties.
- (b) Awardee includes Proposed Awardee and means the person or entity that was a successful Bidder to a Solicitation and has been, or is intended to be, awarded the contract.
- (c) Close of Business, as used in this chapter, means 5 p.m. Pacific Standard Time (PST) or Pacific Daylight Time (PDT), as applicable.
- (d) Contracting Department means either Procurement or the department which has applied and been approved by the Department of General Services to conduct the Solicitation under the Alternative Protest Pilot Project (Public Contract Code sections 12125-12130.).
- (e) Coordinator means the person designated as the Alternative Protest Pilot Project Coordinator by the Department of General Services, Procurement Division, to coordinate all aspects of the Solicitation under the Alternative Protest Pilot Project (Public Contract Code sections 12125-12130).
- (f) Estimated Contract Value means the value of Protestant's bid.
- (g) Frivolous means a protest with any or all of the following characteristics:
 - (1) It is wholly without merit.
 - (2) It is insufficient on its face.
 - (3) The Protestant has not submitted a rational argument based upon the evidence or law which supports the protest.
 - (4) The protest is based on grounds other than those specified in section 1410.
- (h) Major Information Technology Acquisition means the purchase of goods or services, or both, by a state agency, through contract, from non-governmental sources, that has significant mission criticality, risk, impact, complexity, or value attributes or characteristics. Pursuant to subdivision (e) of Section 11702 of the Government Code, these purchases shall include, but not be limited to, all electronic technology

systems and services, automated information handling, system design and analysis, conversion of data, computer programming, information storage and retrieval, telecommunications that include voice, video, and data communications, requisite system controls, simulation, electronic commerce, and all related interactions between people and machines.

- (i) OAH means the Department of General Services, Office of Administrative Hearings.
- (j) Party means the Procurement Division of the Department of General Services, the Contracting Department, the Awardee, and Protestant(s).
- (k) Procurement means the Procurement Division of the Department of General Services.
- (l) Protestant means a person or entity that was an unsuccessful Bidder to a Solicitation under the Alternative Protest Pilot Project (Public Contract Code sections 12125-12130) and that protests the award.
- (m) Small Business means a Certified California Small Business, pursuant to Government Code Division 3, Part 5.5, Chapter 6.5 (commencing with section 14835) and Title 2, California Code of Regulations, section 1896.
- (n) Solicitation means the document that describes the goods or services to be purchased, details the contract terms and conditions under which the goods or services are to be purchased, and establishes the method of evaluation and selection.
- (o) Solicitation File means the Solicitation and the documents used by the Contracting Department in the Solicitation process, including documents used to evaluate Bidders and select a Proposed Awardee. The Solicitation File shall remain available to the public except information that is confidential or proprietary.

Authority cited: Section 12126, Public Contract Code. Reference: Section 11702, Government Code; and Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1404. Notice of Intent to Award Contract.

The Contracting Department shall post a Notice of Intent to Award Contract in a public place specified in the Solicitation, send rejection facsimiles to rejected Bidders, and send Notice of Intent to Award Contract facsimiles to any Bidder who made a written request for notice and provided a facsimile number. The Contracting Department shall indicate that the Solicitation File is available for inspection. The Contracting Department has the discretion to award a contract immediately, upon approval by the Director of the Department of General Services and, if the Solicitation was for a Major Information Technology Acquisition, the Director of the Department of Information Technology.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

Article 2. Protest Procedure

§1406. Notice of Intent to Protest; Service List.

- (a) An unsuccessful Bidder who intends to protest the awarded contract pursuant to this chapter must inform the Coordinator. The Notice of Intent to Protest must be in writing and must reach the Coordinator within the number of days specified in the Solicitation, which shall be not less than 1 working day and not more than 5 working days after the posting of the Notice of Intent to Award Contract, as specified in the Solicitation. Failure to give written notice by Close of Business on that day shall waive the right to protest.
- (b) On the day after the final day to submit a Notice of Intent to Protest, the Coordinator shall make a service list consisting of those Bidders who did submit a Notice of Intent to Protest, the Awardee, and the Contracting Department. The Coordinator shall include addresses and facsimile numbers on this list and shall forward this service list to those Bidders who submitted a Notice of Intent to Protest.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New article 2 (sections 1406-1418) and section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1408. Filing a Protest.

- (a) A protest is filed by the submission of: the Detailed Written Statement of Protest and any exhibits specified in section 1412; a check or money order made payable to the Office of Administrative Hearings for the OAH filing fee of \$50; and the arbitration deposit as specified in subsection (c) or (d) to the Coordinator by the Close of Business on the 7th working day after the time specified in the Solicitation for written Notice of Intent to Protest under section 1406. A copy of the Detailed Written Statement of Protest and exhibits must also be served on all Parties named in the service list as specified in section 1406. A Protestant who fails to comply with this subsection waives Protestant's right to protest.
- (b) Protestant(s) must provide a FAX (facsimile) number. Notification by facsimile is sufficient for service. If the Detailed Written Statement of Protest is sent to the Coordinator by facsimile, Protestant must:
- (1) Verify that the pages sent were all received by the Coordinator; and
 - (2) Remit the required deposit and filing fee to Coordinator by any reasonable means. If sending via carrier, the postmark date or equivalent shall be used to determine timeliness.
- (c) Each Protestant not certified as a Small Business shall make a deposit of the estimated arbitration costs, by check or money order made payable to the Office of Administrative Hearings, as determined by the Estimated Contract Value.
- (1) For contracts up to \$100,000.00, the deposit shall be \$1500.00.
 - (2) For contracts of \$100,000.00 up to \$250,000.00, the deposit shall be \$3,000.00.
 - (3) For contracts of \$250,000.00 up to \$500,000.00, the deposit shall be \$5,000.00.
 - (4) For contracts of \$500,000.00 and above, the deposit shall be \$7,000.00.
- (5) Failure to remit a timely required deposit waives the right of protest.
- (6) Any refund to Protestant(s) shall be made per section 1436.
- (d) Each Protestant certified as a Small Business shall submit a copy of the Small Business Certification in lieu of the deposit specified in subsection (c). If Protestant is a Small Business and the protest is denied by the arbitrator, the Contracting Department shall collect the costs of the arbitration from Protestant. If Protestant does not remit the costs due, the Contracting Department may offset any unpaid arbitration costs from other contracts with Protestant and/or may declare Protestant to be a non-

responsible Bidder on subsequent solicitations.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1410. Grounds for Protest.

- (a) The Public Contract Code, at section 12126(d) provides: Authority to protest under this chapter shall be limited to participating Bidders.
 - (1) Grounds for Major Information Technology Acquisition protests shall be limited to violations of the Solicitation procedures and that the Protestant should have been selected.
 - (2) Any other acquisition protest filed pursuant to this chapter shall be based on the ground that the bid or proposal should have been selected in accordance with selection criteria in the Solicitation document.
- (b) The burden of proof for protests filed under this chapter is preponderance of the evidence, and Protestant(s) must bear this burden.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1412. Detailed Written Statement of Protest.

- (a) The Detailed Written Statement of Protest must include the grounds upon which the protest is made, as specified in 1410(a).
- (b) The Detailed Written Statement of Protest shall contain reasons why Protestant should have been awarded the contract.
 - (1) For Major Information Technology Acquisition protests, the Detailed Written Statement of Protest must specify each and every Solicitation procedure which was violated and the manner of such violation by specific references to the parts of the Solicitation attached as exhibits and why, but for that violation, Protestant would have been selected.
 - (2) For other acquisition protests, the Detailed Written Statement of Protest must specify each and every selection criterion on which Protestant bases the protest by specific references to the parts of the Solicitation attached as exhibits.
 - (3) For all protests, Protestant must specify each and every reason that all other Bidders who may be in line for the contract award should not be awarded the contract.
- (c) The Detailed Written Statement of Protest must be limited to 50 typewritten or computer generated pages, excluding exhibits, at a font of no less than 12 point or pica (10 characters per inch), on 8 1/2 inch by 11-inch paper of customary weight and quality. The color of the type shall be blue-black or black. In addition to a paper copy, the arbitrator may request that a Protestant submit such information on computer compatible diskette or by other electronic means if the Protestant has the ability to do so.
- (d) Any exhibits submitted shall be paginated and the pertinent text highlighted or referred to in the Detailed Written Statement of Protest referenced by page number, section and/or paragraph and line number, as appropriate.

-
- (e) The Detailed Written Statement of Protest shall not be amended.
 - (f) Protestant(s) may not raise issues in hearing which were not addressed in the Detailed Written Statement of Protest.
 - (g) A Protestant who fails to comply with this subsection waives Protestant's right to protest.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1414. Review by Coordinator.

- (a) Within 2 working days after receipt of the Detailed Written Statement of Protest, the Coordinator shall notify the Contracting Department and the Awardee of a potential protest hearing.
- (b) The Coordinator shall review the Detailed Written Statement of Protest within 5 working days after receipt to preliminarily determine if the protest is Frivolous and notify Protestant of the option to withdraw or proceed in arbitration.
 - (1) If Protestant withdraws the protest within 2 working days after the notification by the Coordinator of a preliminary determination of Frivolousness, the Coordinator shall withdraw the preliminary finding of Frivolousness and refund Protestant's deposit and filing fee.
 - (2) If the Protestant previously filed two protests under the Alternative Protest Pilot Project preliminarily determined Frivolous by the Coordinator but then withdrew or waived them before the arbitration decision, the Coordinator shall make final the preliminary determination of Frivolousness for the Department of General Services.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1416. Review and Response by Contracting Department and Awardee.

- (a) The Awardee shall have 7 working days after notification by the Coordinator to submit to the Coordinator and Protestant a response to the Detailed Written Statement of Protest.
- (b) The Contracting Department, in conjunction with the Coordinator, shall have 7 days after the filing of the Detailed Written Statement of Protest to send a response to Protestant and Awardee.
- (c) Responses shall follow the standards set forth in section 1412(c) and (d).

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1418. Bond Requirement.

- (a) If the Coordinator has determined that a protest is Frivolous and the Protestant does not withdraw the protest, the Protestant shall be required to post a bond in an amount not less than 10% of the

Estimated Contract Value.

- (b) The percentage of the bond shall be determined by the Contracting Department and specified in the Solicitation.
- (c) Protestant shall post the bond, pursuant to Chapter 2 (commencing with section 995.010) of Title 14 of Part 2 of the Code of Civil Procedure, within 15 working days of the filing of the Detailed Written Statement of Protest or shall be deemed to have waived the right to protest.
- (1) If the arbitrator determines that the protest is Frivolous, the bond shall be forfeited to Procurement and the Coordinator will impose Sanctions.
- (2) If the arbitrator determines that the protest is not Frivolous, the bond will be returned to the Protestant and no Sanctions imposed.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 995.010 et. seq., Code of Civil Procedure; and Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

Article 3. Arbitration Procedure

§1420. Arbitration Process.

Within 19 calendar days after the Notice of Intent to Award has been posted, the Coordinator shall consolidate all remaining protests under the Solicitation, and send to OAH:

- (a) a copy of all Detailed Written Statements of Protest;
- (b) OAH filing fees;
- (c) arbitration deposits, and/or notice that any Protestant is a Small Business;
- (d) Awardee responses;
- (e) Coordinator/Contracting Department responses;
- (f) the Solicitation File; and
- (g) notice to OAH whether interpreter services will be needed for any Protestant or Awardee. OAH shall arrange interpreter services which shall be paid by the Contracting Department.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New article 3 (sections 1420-1440) and section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1422. Selection of Arbitrator.

- (a) Within 2 working days after receipt of the protest from the Coordinator, OAH shall furnish the names of ten arbitrators to Protestant(s), the Awardee, and the Coordinator. The arbitrator list shall include administrative law judges who are employees of OAH and contract private arbitrators who are not employees of the State of California. Protestant(s), the Awardee, and the Coordinator may each strike two of the ten names and notify OAH within 2 working days. Protestant(s) may also indicate if they prefer a contract arbitrator or an OAH administrative law judge. OAH may then select as arbitrator any name not stricken and shall notify Protestant(s), the Awardee, and the Coordinator within 2 working days. If all names

are stricken, the Director of OAH shall appoint an arbitrator.

(b) A proposed arbitrator shall be disqualified on any of the grounds specified in Section 170.1 of the Code of Civil Procedure for the disqualification of a judge.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1424. Authority of Arbitrator.

(a) Arbitrators are authorized to:

- (1) Administer oaths and affirmations;
- (2) Make rulings and orders as are necessary to the fair, impartial, and efficient conduct of the hearing; and
- (3) Order additional deposits from Protestant(s) to cover additional estimated costs. If OAH does not receive the required deposit(s) in the time specified, the right to protest will be deemed waived.

(b) The arbitrator shall have exclusive discretion to determine whether oral testimony will be permitted, the number of witnesses, if any, and the amount of time allocated to witnesses.

(c) It shall be in the arbitrator's exclusive discretion to determine whether to:

- (1) Conduct a prehearing conference; and/or
- (2) Permit cross-examination and, if so, to what extent; and/or
- (3) Review documents alone for all or part of the protest.

(d) It shall be in the arbitrator's exclusive discretion to determine whether additional responses and rebuttals are to be submitted, and the timelines and page limits to be applied.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1426. Decision Based in Whole or in Part on Documents Alone.

Any Party may request that the arbitrator base the arbitrator's decision on documents alone. It shall be the arbitrator's exclusive discretion to do so.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1428. Prehearing Conference.

(a) If the arbitrator determines that a prehearing conference is necessary, OAH shall set the time and place and notify Protestant(s), the Awardee, and Procurement at least 5 working days prior to the prehearing conference.

(b) The prehearing conference shall be held to identify and define issues in dispute and expedite the arbitration. The parties should be prepared to discuss, and the arbitrator may consider and rule on, any of the following matters applicable to the protest:

- (1) Clarification of factual and legal issues in dispute as set forth in the Detailed Written Statement of Protest.
- (2) The extent to which testimony shall be permitted and the extent to which cross-examination will be allowed.
- (3) Identity of and limitations on number of witnesses, need for interpreters, scheduling and order of witnesses, etc.
- (4) Any other matters as shall promote the orderly and efficient conduct of the hearing.
- (c) At the prehearing conference, Protestant(s), the Awardee, and Procurement shall deliver a written statement which contains the name of each witness a party wishes to call at hearing along with a brief written statement of the subject matter of the witness's expected testimony. If the arbitrator, in his or her exclusive discretion, allows an expert witness to be called, the party calling the witness shall provide the name and address of the expert along with a brief statement of the opinion the expert is expected to give. The party shall also attach a statement of qualifications for the expert witness.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1430. Scheduling the Hearing.

The arbitrator shall schedule the date, time, and place of hearing and notify all Parties.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1432. Discovery.

The arbitrator has exclusive discretion to issue subpoenas and/or subpoena duces tecum. There shall be no right to take depositions, issue interrogatories, or subpoena persons or documents.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1434. Attendance at Hearings.

The Arbitration hearings shall be open to the public unless the arbitrator, in his or her exclusive discretion, determines that the attendance of individuals or groups of individuals would disrupt or delay the orderly conduct or timely completion of the proceedings.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

-
1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1436. Arbitrator's Decision.

- (a) The final decision shall be in writing and signed by the arbitrator. It shall include a Statement of the Factual and Legal Basis for the decision, addressing the issues raised in the Detailed Written Statement(s) of Protest, and shall include an order upholding or denying the protest(s). The arbitrator's order shall not award a contract.
- (b) A copy of the decision shall be sent by regular mail to Procurement, the Contracting Department, the Awardee, and Protestant(s) within 45 calendar days after the filing of the first Detailed Written Statement of Protest. In the arbitrator's exclusive discretion, this timeline may be extended for an additional 15 calendar days. The arbitrator's failure to issue a decision within the time specified by this section shall not be a ground for vacating the decision.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1437. Costs.

- (a) For protests not determined Frivolous by Procurement:
 - (1) If the arbitrator denies the protest, Protestant(s) will be liable for all costs of the arbitration.
 - (2) If the arbitrator upholds the protest, the Contracting Department shall pay for all costs of the arbitration and Protestant(s) will be refunded the deposit by OAH.
- (b) If Procurement determined that the protest was Frivolous and the arbitrator affirms that the protest is Frivolous, the bond shall be forfeited to Procurement, the protest will be denied, and Protestant(s) will be liable for all costs of the arbitration.
- (c) If Procurement determined that the protest was Frivolous and the arbitrator determines that the protest is not Frivolous, any bond(s) posted by Protestant(s) shall be returned:
 - (1) If the arbitrator denies the protest, Protestant(s) shall be liable for half of the costs of the arbitration. The Contracting Department shall pay the remaining half of the arbitration costs.
 - (2) If the arbitrator upholds the protest, the Contracting Department shall pay for all costs of the arbitration and Protestant(s) will be refunded the deposit by OAH.
- (d) A Protestant who withdraws his or her protest before the arbitrator's decision has been issued will remain liable for all arbitration costs up to the time of withdrawal. These costs include, but are not limited to, the arbitrator's time in preparation, prehearing conferences, and hearing the protest. If Procurement deemed the protest Frivolous, any bond posted shall be forfeited to Procurement.
- (e) Except as provided in (f), if any costs are determined to be payable by Protestant(s), that amount shall be subtracted from deposit(s) of Protestant(s) as ordered by the arbitrator. Any additional costs shall be billed to Protestant(s) and any refunds shall be sent to Protestant(s) by OAH.
- (f) If a Protestant is a Small Business, then the Contracting Department shall pay OAH all arbitration costs and collect the amount due from Protestant.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract

Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1438. Judicial Review.

The grounds for judicial review shall be as set forth in Chapter 4 of Title 9 of Part III of the Code of Civil Procedure (commencing with section 1285).

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).

§1440. Transcripts.

(a) A party desiring a transcript of the proceedings shall contact the OAH Transcript Clerk to make arrangements to pay for preparation of the transcript. Prior to preparation of the transcript, a deposit equal to the estimated cost of the transcript shall be paid. Preparation of the transcript will be arranged by the OAH Transcript Clerk. The deposit shall be applied to the actual cost and any excess shall be returned to the party that submitted the request. Any balance due shall be paid by the party or a representative on behalf of the party requesting the transcript before the transcript is released to the requesting party.

(b) Unless a record of a proceeding or any portion thereof was sealed, any person may request a transcript or a recording of the proceeding. If a record of a proceeding or any portion thereof was sealed, only parties to the proceeding may request a transcript of the sealed portions, and the sealed portions shall not be disclosed to anyone except in accordance with the order sealing the proceeding or subsequent order.

Authority cited: Section 12126, Public Contract Code. Reference: Sections 12125-12130, Public Contract Code.

1. New section filed 8-18-98; operative 8-18-98 pursuant to Government Code section 11343.4(d) (Register 98, No. 34).
-

ATTACHMENT 4 – SOLICITATION SUBMISSION CHECKLIST

(This Attachment is not required to be submitted with your solicitation response.)

Has your firm submitted the following pre-bid information?

- Exhibit 2, Intent to Bid
- Exhibit 3, Confidentiality Statement

Does your Final Bid follow the format specified in Section 6?

- Packaged and labeled as identified in Section 6.
- Provided in the number of copies and formatted as identified in Section 6.
- No cost data provided in any volumes, except Volume 3.

Is your Final Bid provided in the following order, as identified in Section 6?

Volume 1 – Response to Administrative, and Qualifications

- Cover letter with original signature and information specified in Section 3.9
- Exhibit 4: Response to Administrative Requirements
- Exhibit 5: GSPD 05-105 Bidder Declaration
- Exhibit 6: Secretary of State Certification
- Exhibit 7: Workers’ Compensation Certification
- Exhibit 8: Seller’s Permit certification
- Exhibit 9: Payee Data Record
- Exhibit 10: Iran Contracting Act of 2010
- Exhibit 12: DVBE Declarations
- Exhibit 13: Bidding Preferences and Incentives
- Exhibit 14: Commercially Useful Function Certification
- Exhibit 18.1 through 18.2, Bidder’s Qualifications Form(s) and Bidder’s Reference Form(s)
- Exhibit 19.1 through 19.8, Staff Qualifications Forms and Staff’s Reference Forms

- Exhibit 20: Requirements Certification
- Exhibit 21: Proposal Narrative Requirements
- Exhibit 22: Cost Worksheets
- Exhibit 23: Bidder’s Library

Preference/Incentive Exhibits (required only as indicated)

- Exhibit 15: STD 830, TACPA Preference Request (required if claiming TACPA preference)

Volume 2 – STD 213, Standard Agreement with Statement of Work attached

- Exhibit 1: STD 213, Standard Agreement
- Statement of Work

Volume 3 – Cost Information – Exhibit 22

- Cost Worksheet #1 – Main Menu
- Cost Worksheet #5-1 – Cost Evaluation
- Cost Worksheet #5-2 – Contract Cost
- Cost Worksheet #5-3 – Labor Rates
- Cost Worksheet #5-4 – Labor Costs
- Cost Worksheet #5-5 – Software Costs

The State makes no warranty that the checklist is a full and comprehensive listing of every requirement specified in the solicitation. Checking off the items on the checklist does not establish your firm’s intent nor does it constitute responsiveness to the requirements. The checklist is only a tool to assist participating Bidders in compiling the Final Bid response. Bidders are encouraged to carefully read the entire solicitation. The need to verify all documentation and responses prior to the submission of Final Bids cannot be over emphasized.

MAIN MENU

Bidder:	
---------	--

Assumptions:

Period	# of Weeks	# of Sprints	# of Weekly Labor Hours
Base Period	12	6	45
Optional 1	12	6	45
Optional 2	14	7	45
Optional 3	14	7	45

The following table can be used to navigate between cost worksheets.

Cost Worksheet Navigation:

- Worksheet 5-1 Cost Evaluation
- Worksheet 5-2 Contract Cost
- Worksheet 5-3 Labor Rates
- Worksheet 5-4 Labor Costs
- Worksheet 5-5 Software Costs

COST EVALUATION

Cost Category	Total Bid
Labor Costs (Worksheet 5-4)	\$ -
Software Costs (Worksheet 5-5)	\$ -
COST EVALUATION TOTAL	\$ -

CONTRACT COST

Cost Category	Base Period	Optional 1	Optional 2	Optional 3	Total Contract
Labor Costs (Worksheet 5-4)	\$ -	\$ -	\$ -	\$ -	\$ -
CONTRACT TOTAL	\$ -				

State of California Office of Systems Integration

Appendix C, Cost Workbook 7-3 Labor Rates

RFP OSI #31326
CWS-NS Project

LABOR RATES

PROCUREMENT CONFIDENTIAL

LABOR COSTS

SOFTWARE COSTS

Software Name/Product Number/Version	License Type	Qty.	Unit Cost	Total Unit Maint. Cost	Extended Cost	Extended Maint.	Total Cost
				\$ -	\$ -	\$ -	\$ -
				\$ -	\$ -	\$ -	\$ -
				\$ -	\$ -	\$ -	\$ -
				\$ -	\$ -	\$ -	\$ -
				\$ -	\$ -	\$ -	\$ -
				\$ -	\$ -	\$ -	\$ -
				\$ -	\$ -	\$ -	\$ -
				\$ -	\$ -	\$ -	\$ -
				\$ -	\$ -	\$ -	\$ -
Software Total					\$ -	\$ -	\$ -

CWS-NS API RFP OSI # 31801 – EXHIBIT 21 – NARRATIVE REQUIREMENTS FOR API

EXHIBIT 21 – NARRATIVE REQUIREMENTS FOR API

Req ID#	Requirement Description	Narrative Response	Maximum Score
1	The Bidder shall describe their technical approach that reflects a clear understanding of the technical challenges associated with development of the Intake module, including the use of RESTful APIs, development framework, and system administration practices.		250
2	The Bidder shall describe their user interaction approach, including user research, user interviews, and 1:1 task based usability testing; product identification and research; user behaviors, needs, and motivations; testing metrics and narrative.		90
3	The Bidder shall describe their project management approach using its proposed Agile methodology.		90
4	The Bidder shall submit a Product Development Roadmap and include as an attachment.	To be included as a separate attachment to Bidder's response.	90
5	The Bidder shall describe their approach for developing sprint artifacts, including artifacts related to builds, testing, training, security, and cut-over planning.		90

CWS-NS API RFP OSI # 31801 – EXHIBIT 21 – NARRATIVE REQUIREMENTS FOR API

Req ID#	Requirement Description	Narrative Response	Maximum Score
6	The Bidder shall describe their Quality Control and Performance Measurement approach, including how proposed performance standards will be monitored, evaluated, and reported.		90

EXHIBIT A – STATEMENT OF WORK**REQUEST FOR PROPOSAL****1. PURPOSE**

This Statement of Work (SOW) reflects the services to be provided by <Contractor Name>, hereinafter referred to as the “Contractor,” for the State. This SOW is governed by and incorporates by reference the terms and conditions attached herein.

This SOW describes the creation of an Application Program Interface (API) to encapsulate the existing CWS/CMS (Child Welfare Services/Case Management System)¹ to enable rapid and modern development of new user facing software modules. The API will replicate and extend the business rules currently implemented in the CWS/CMS client and server Visual Basic 6 (VB6) and COBOL source code in order to create a collection of RESTful JSON interfaces that allow new modules to extend and interoperate with CWS/CMS.

API Product Vision and Background**The Legacy System**

The CWS/CMS is a 20 year old system with usability, maintenance, and data accuracy issues. The system was originally developed to meet the needs of users to assure the safety, permanency and well-being of children at risk of abuse, neglect or exploitation. CWS is dedicated to modernizing and improving this business functionality. It is used by each of the 58 county child welfare and probation agencies, Title IV-E Tribes, and the State of California. Business function automation will be modernized one module at a time, with modernization including replacing and extending existing functionality.

The API Module

This RFP focuses on the creation of an API encapsulating the existing system to enable rapid and modern development of the modules. The first customer facing module to be developed (by a State-provided vendor) is the Intake module. The Intake module is an important initial entry point into child welfare services and includes processes to receive referrals from community members and mandatory reporters, as well as conduct investigations of abuse and neglect. This first module will be a consumer of the API.

Future modules slated for modernization are (and will eventually be supported by this API):

¹ <http://www.childsworld.ca.gov/PG1328.htm>

- Children's residential licensing
- Case management
- Resource management
- Court processing
- Eligibility
- Financial management
- Administration

Eventually, over time the existing database and system will be decommissioned and this new API will be used for all continuing development.

The high level goals of the RFP are the following:

- Create a RESTful API using standard open protocols such as JSON or XML.
- Create the API to read/write to the existing database (for existing data fields and tables) and also read/write to a new database (for new data fields and tables).
- Achieve comprehensive test coverage of existing legacy interface, so future refactoring efforts are easier.

Existing System

Currently, the back-end of the Child Welfare system runs on 2 IBM mainframes in a sysplex at the California Department of Technology Gold Camp data center facility. The database, DB2, interacts with an application layer written primarily in COBOL. The business logic -- including data validation -- exists both at the application layer and at the thick client. Currently, there are approximately 200+ business rules at the application layer. (Detailed documentation is available in the Bidders' Library).

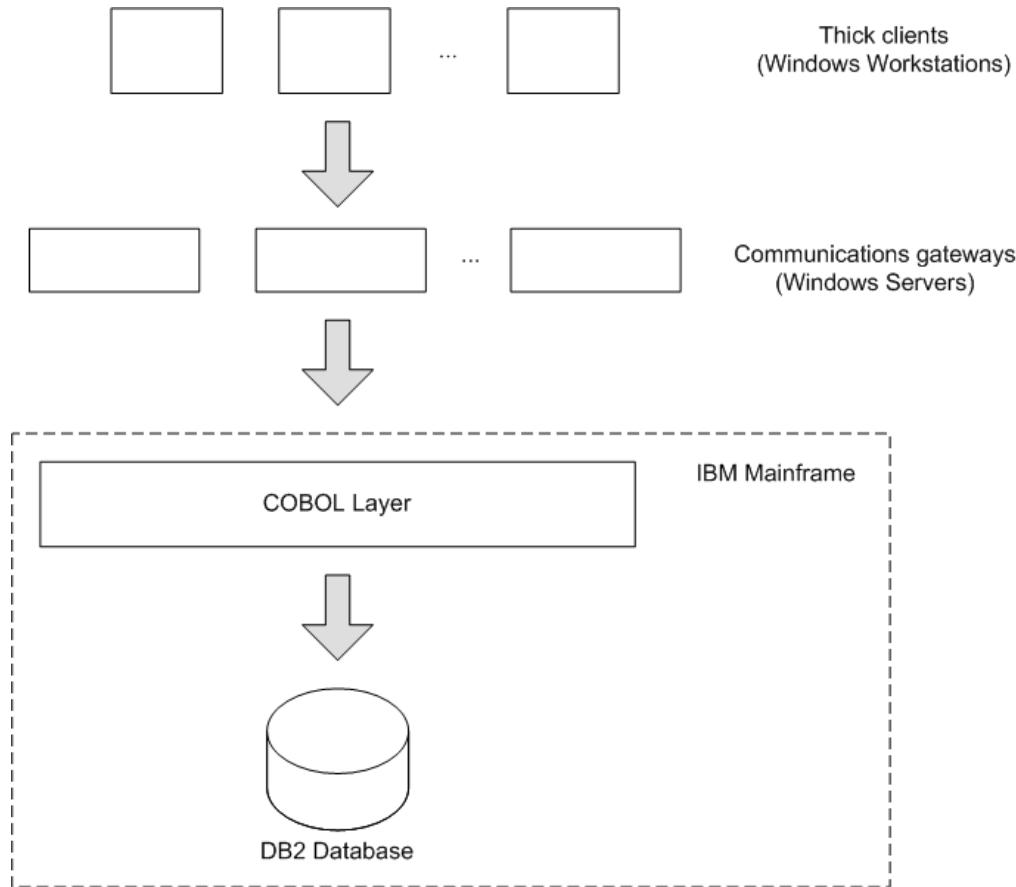


Figure 1: A simple high level view of the existing system. The COBOL layer and thick clients contain business logic.

2. TERM

- a. The term of this Agreement shall commence on **MM/DD/YYYY**, or the date the Agreement is executed by both parties, whichever is later, **MM/DD/YYYY** and continue through **MM/DD/YYYY**.
- b. Effective upon approval of the California Department of Technology Procurement Division (STPD), the term of the Agreement is for three (3) month base period with three (3) additional three (3) month terms executed at the State's sole option.
- c. The Contractor shall not be authorized to deliver goods or commence performance of services described in this Agreement prior to the Effective Date. Any delivery of goods or performance of services by the Contractor that is commenced prior to the Effective Date shall be considered gratuitous on the part of the Contractor.

3. WORK LOCATION

The Contractor is required to perform all services under this Agreement onsite at the state facility in Sacramento, CA. The CWS-NS Project is located at 744 P Street, Sacramento, CA 95814.

4. COST

The total cost of this Agreement is **<to be completed at contract award>**. The costs associated with each Fiscal Year are approximate and may be redirected between Fiscal Years without the requirement of a Contract amendment.

5. SCOPE OF SERVICES

- 5.1. The Contractor shall provide the following services and artifacts for the development of the API module.

Sprint Zero Artifacts

- 5.2. The Contractor shall produce, review and written agreement from the State for all Sprint Zero artifacts prior to commencing delivery sprints.
- 5.3. The Contractor shall produce a User Story Definition and Acceptance Criteria Format.
- 5.4. The Contractor shall produce Coding Standards (including style guidelines) and Commenting Standards, including Peer Review checklist.
- 5.5. The Contractor shall produce a Sprint-level Definition of Done that includes the following concepts:
 - a. Code produced (all 'to do' items in code completed)
 - b. Code commented, checked in and run against current version in source control
 - c. Peer reviewed (or produced with pair programming) and meeting development standards
 - d. Builds without errors
 - e. Unit tests written and passing
 - f. Deployed to system test environment and passed system tests
 - g. Passed Product Owner Acceptance Testing
 - h. Any build/deployment/configuration changes Implemented/documentied/communicated
 - i. Relevant documentation produced/updated (e.g., how the API services supports service module needs and user stories, user stories, sketches, wireframes, clickable prototypes)
 - j. Remaining hours for task set to zero and task closed

- 5.6. The Contractor shall produce a Release-level Definition of Done that includes the following concepts:
 - a. Release Notes Prepared
 - b. Deployed to staging environment and integration, performance and load tests run
 - c. Relevant documentation/diagrams produced and/or updated

Sprint Planning and Execution

- 5.7. The Contractor shall use an Agile Sprint Planning and User Story Approval process for each Sprint. The Agile Sprint Planning process includes the following activities: Product Backlog refinement, User Story creation, estimation and commitment.
- 5.8. The Contractor shall demonstrate that each User Story has met the definition of done so that the State Product Owner can approve each User Story as it is completed.
- 5.9. The Contractor shall utilize scrum-based agile processes in sprint execution activities (e.g., User Story development, Product Backlog maintenance, User Story acceptance, Retrospective, and Product Review).
- 5.10. The Contractor shall revise Sprint Zero artifacts during each Sprint Retrospective process, as appropriate.
- 5.11. The Contractor shall generate documentation within the code itself and within the version control system (e.g., through proper use of descriptive commit messages, issue tracking, pull requests, etc.).
- 5.12. The Contractor shall use Pivotal Tracker to manage the Product Backlog, User Story acceptance, and maintain a scrum board.
- 5.13. The Contractor shall use Slack as the primary mechanism for project-related communication and real-time messaging, archiving and search for all project teams.
- 5.14. The Contractor shall provide a report at the conclusion of each sprint that documents the planned user stories, accepted user stories, open impediments, and technical debt.
- 5.15. The Contractor shall adhere to Twelve-Factor Application design constraints (see <http://12factor.net/>).

Modularity

- 5.16. The Contractor shall design the application architecture to ensure a separation of concerns and a reasonable degree of modularity between systems.
- 5.17. The Contractor shall adhere to the DRY (Don't Repeat Yourself) principle to ensure that the codebase remains flexible.

Code Style

- 5.18. The Contractor shall ensure that all code will be written to a language specific code-style guideline (e.g., PEP8 for Python).
- 5.19. The Contractor shall use an automated tool to evaluate the codebase and ensure compliance with the code-style guideline (e.g., if the Contractor uses Python, PyLint may be used).

Version Control System

- 5.20. The Contractor shall manage all assets (e.g., source code, automated tests, user stories, configuration files, knowledge transfer material, etc.) using GitHub.

Code Review

- 5.21. The Contractor shall ensure all code written by one developer is reviewed by another developer before merging into the mainline codebase.
- 5.22. The Contractor shall follow industry standard code review practices (e.g., <http://blog.fogcreek.com/increase-defect-detection-with-our-code-review-checklist-example/>).

Automated Testing

- 5.23. The Contractor shall create and execute automated unit testing.
- 5.24. The Contractor shall create and execute automated system tests to verify all Features of the software module.

- 5.25. The Contractor shall create and execute automated Product Owner Acceptance testing to verify all user facing functionality.
- 5.26. The Contractor shall run tests automatically on code merged into version control.
- 5.27. The Contractor shall use an automated tool that measures the amount of the codebase that is covered by tests (e.g., RCov may be used to measure test coverage of Ruby code).
- 5.28. The Contractor shall create and execute automated integration testing with other contractor developed modules.
- 5.29. The Contractor shall make the bugs identified during testing available to view real-time and on a historical basis.

Load Tests

- 5.30. The Contractor shall create and execute load and performance tests at regular intervals, and at each release.
- 5.31. The Contractor shall provide a summary of all load and performance test results.

Accessibility

- 5.32. The Contractor shall incorporate and test accessibility throughout the design and development processes (see section 508 Amendment to the Rehabilitation Act of 1973).
- 5.33. The Contractor shall use an automated accessibility testing tool (e.g., Pa11y).

Issue Tracking

- 5.34. The Contractor shall use GitHub to keep track of all bugs and application issues.

Mobile Friendly

- 5.35. The Contractor shall design the User Interface (UI) using responsive design.

Logging and Monitoring

- 5.36. The Contractor shall implement centralized and continuous monitoring.

5.37. The Contractor shall implement centralized system logging.

5.38. The Contractor shall implement auditing.

Security

- 5.39. The Contractor shall use an automated black/white box security scanning tool (e.g., HP Fortify, or <https://hakiri.io>) to ensure a minimal baseline of security at regular intervals, and at each release.
- 5.40. The Contractor shall provide the results of the security scans to the State.
- 5.41. The Contractor must adhere to the HTTPS-Only Standard as outlined in <https://https.cio.gov/>.
- 5.42. The Contractor shall adhere to the baseline moderate tailored NIST 800-53 (see Attachment).
- 5.43. The Contractor shall ensure adequate security controls using penetration testing, red teaming, etc.

User Authentication and System Administration

- 5.44. The Contractor shall ensure that the module integrates with the existing authentication protocols, which involves Active Directory and IBM's RACF technology.
- 5.45. The Contractor shall enable external service authentication and authorization using a modern single sign-on tool (e.g., Shibboleth and OAuth 2.0).

Build and Deployment

- 5.46. The Contractor shall provide continuous integration of source code into the source code version control system.
- 5.47. The Contractor shall use a continuous source code build tool that enables continuous deployment of all applications into testing and staging environments.

- 5.48. The Contractor shall include mock test data that should be publicly accessible for development by other module Contractors and not include personally identifiable information (PII).
- 5.49. The Contractor shall use at least one of the following methods to deploy code changes to a staging environment under the control of the Contractor with the issuance of a single command:
 - a. Containerization (e.g., Docker Engine, Rkt, and Warden)
 - b. Configuration Management tools (e.g., Chef, Puppet, Salt, and Ansible)
- 5.50. The Contractor shall submit server images to State using a Deployment/Release tool at the conclusion of each sprint and upon major releases.

API Specific Scope of Work

The required approach is to execute the work in phases that will occur during the base and optional periods. The first phase is to encapsulate and proxy the existing COBOL layer as a RESTful, JSON API. The second phase is modify the API to support the Intake module and introduce a new database to store the new fields and tables necessary.

Phase 1

During this phase the Contractor will develop a RESTful API that mirrors legacy Intake business and data access logic.

- 5.51. The Contractor shall extract the legacy Intake business logic from the desktop VB6 thick client application and the legacy data access logic from the COBOL interface layer.
- 5.52. The Contractor shall implement the legacy system logic in the RESTful web API.
- 5.53. The Contractor shall ensure that system and database activity logging are compatible with methods used by CWS/CMS.

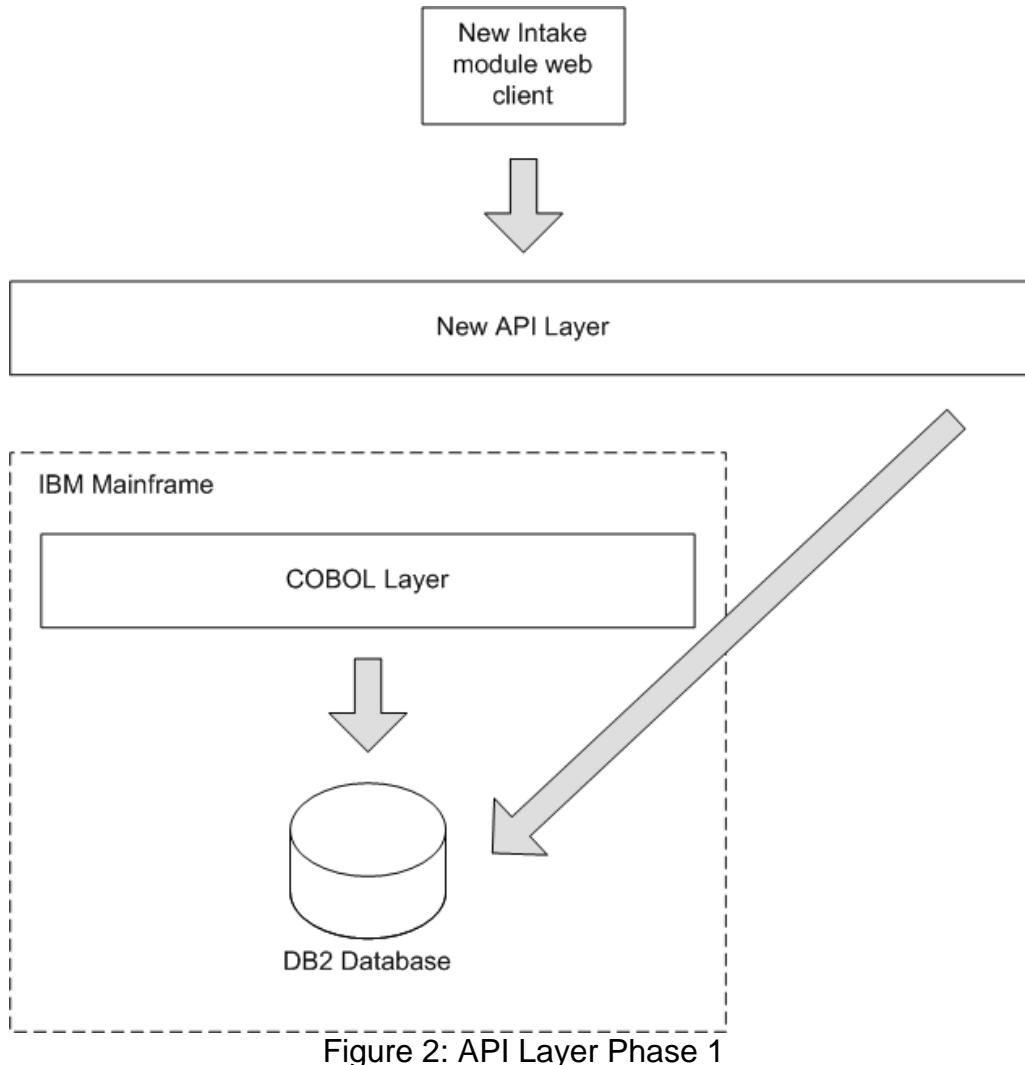
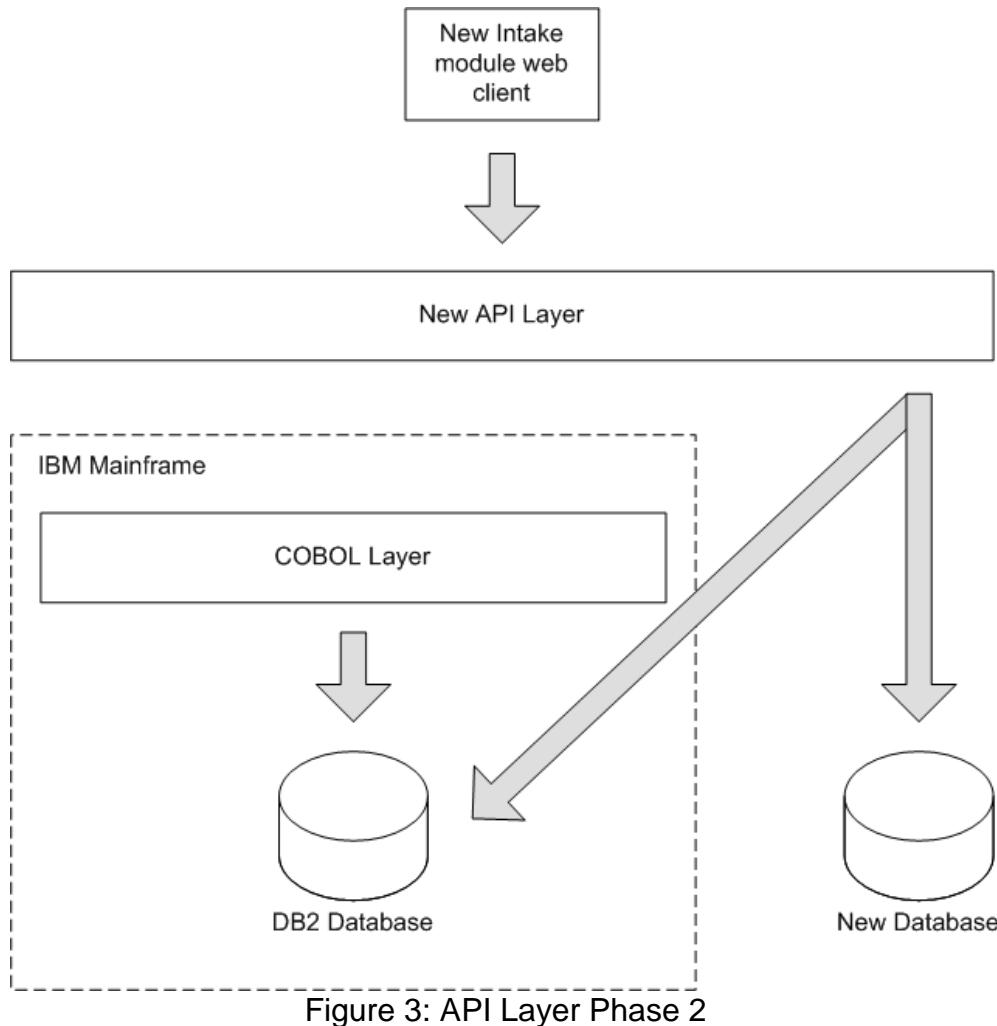


Figure 2: API Layer Phase 1

Phase 2

During this phase, the Contractor will modify the new API to align with the new Intake module's business functionality.

- 5.54. The Contractor shall store new data fields and tables identified for the Intake module in a new database.
- 5.55. The Contractor shall develop the API to simultaneously read and write new data fields to the new database and old data fields to the DB2 database (as appropriate).
- 5.56. The Contractor shall utilize a SQL compliant database to support the new database.



6. Deliverables and Due Dates

The deliverables and due dates for this Contract are as follows.

Deliverable	Deliverable Description	Due Date
Sprint Status Report	Identifies the planned user stories, accepted user stories, open impediments, and newly accumulated or resolved technical debt.	Conclusion of each sprint

7. PERSONNEL AND RATES

The personnel shall perform the tasks described in this SOW, at the rates indicated in the Agreement.

- 1) Given the size, scope, and complexity of this project, it is of utmost importance that the individual(s) have adequate hours to work effectively on this Project. The Contractor shall be responsible for monitoring the monthly hours billed to ensure the individual(s) effectively meet(s) the needs of the Project.
- 2) The assigned individual(s) will perform the tasks described in this SOW, at the rates indicated in Exhibit 22, Cost Worksheet. The Contractor shall identify each individual by name, labor category, and hourly rate.
- 3) Contractor shall provide an Organization Chart identifying each of the proposed team members. Refer to Attachment III-B, Vendor Organization Chart.

a. KEY PERSONNEL

The key personnel specified in this contract are considered to be essential to work performance. At least 15 calendar days before changing any identified individual to other programs or contracts (or as soon as possible, if an individual must be replaced, for example, as a result of leaving the employ of Contractor), Contractor shall notify the State Project Director and shall submit comprehensive justification for the diversion or replacement request (including proposed substitutions for key personnel) to permit evaluation by the State of the effect on performance under this contract. Contractor shall not divert or otherwise replace any key personnel without the written consent of the State Project Manager.

The State may modify the contract to add or delete key personnel at the request of the Contractor or State.

1. The Contractor agrees that the key personnel shall not be removed from the contract effort, replaced or added to the contract without a compelling reason and without compliance with paragraph (2) hereof. The State will not approve substitutions for the sole convenience of Contractor.
2. If any change to the key personnel position becomes necessary (substitutions or additions), the Contractor shall immediately notify the State Project Director in writing, accompanied by the resume of the proposed replacement personnel who shall be of at least substantially equal ability and qualifications as the individuals currently approved for that category.
3. All requests for approval of changes hereunder must be in writing, via email, and provide a detailed explanation of circumstances necessitating the proposed change.
4. The State reserves the right to have the contractor to replace staff at any time, such right will not be exercised unreasonably. The State will notify the Contractor in writing when exercising that right, and will provide the Contractor with the reason for requiring the replacement. In this event, the Contractor must provide a proposed replacement in accordance with the process and deadline specified herein.

8. CONTRACTOR STAFF ROLES, RESPONSIBILITIES AND MANDATORY QUALIFICATIONS

The Contractor shall meet the roles, responsibilities and MQs listed below. All experience used to meet the MQs shall have been where the Contractor had primary responsibility. Refer to Firm Experience Table, Attachment II-F

ROLE	RESPONSIBILITY	MANDATORY QUALIFICATIONS
Management Lead/Account Representative	The Contractor shall provide a Management Lead. A Management Lead shall ensure that all work on this contract complies with contract terms and conditions and shall have access to vendor's corporate senior leadership when necessary. The vendor's management lead shall be the	<ol style="list-style-type: none"> 1. The Management Lead shall have been responsible for the management of a system similar in scope to the Bidder's proposed solution. 2. The Management Lead shall have been involved in and led a minimum of two software development projects similar in scope to the Bidder's proposed solution.

	<p>primary interface with the Contract Manager and shall attend status meetings and ad hoc meetings with stakeholders as required, accompanied by the technical architect when necessary.</p>	<p>3. The Management Lead shall have a baccalaureate degree from an accredited college or university in a related field, or commensurate experience.</p>
Lead Developer	<p>The Contractor shall provide a Lead Developer. A Lead Developer is primarily responsible for the architecture and design of the subsystems within the Agile Team's purview, subject to approval by the Product Owner. The Lead Developer is responsible for choosing the direction of the Agile Team to execute the Product Owner's vision and goals, and to deliver working software at the end of a sprint. The Lead Developer also helps develop product roadmaps, backlogs, and measurable success criteria, and writing user stories (i.e., can establish a path to delivery for breaking down stories).</p>	<p>1. The Lead Developer shall have been responsible for the development of a system similar in scope to the Bidder's proposed solution.</p> <p>2. The Lead Developer shall have been involved in and led a minimum of two software development projects similar in scope to the Bidder's proposed solution.</p> <p>3. The Lead Developer shall have a minimum of three years of management experience with software development, design, and the System Development Life Cycle (SDLC) methodologies proposed by the Bidder.</p> <p>4. The Lead Developer shall have a computer science, engineering, or technology-related baccalaureate degree from an accredited college or university, or commensurate experience.</p>
Scrum Master	<p>The Contractor shall provide a Scrum Master. A Scrum Master is primarily responsible to help the team achieve its goals. The Scrum Master assures that the team follows the rules of Scrum, helps the team meet their daily and iteration objectives, works to remove impediments in the organization, helps manage the team's relationships with</p>	<p>1. The Scrum Master shall have been responsible for the management of a system similar in scope to the Bidder's proposed solution.</p> <p>2. The Scrum Master shall have been involved in and led a minimum of two software development projects similar in scope to the Bidder's proposed solution.</p>

	<p>outside stakeholders and facilitates team continuous improvement, and coordinates solution implementation and delivery with other Scrum Masters on the Release train. The Scrum Master should have experience serving as the client's point of contact.</p>	<ul style="list-style-type: none"> 3. The Scrum Master shall hold a certification related to Scrum. 4. The Scrum Master shall have a baccalaureate degree from an accredited college or university in a related field, or commensurate experience.
Product Development Team	<p>The Contractor shall provide an API Product Development Team that consists of 5-7 members. The API Product Development Team shall be a cross-functional development team as appropriate for the sprint and module.</p>	<ul style="list-style-type: none"> 1. Each member of the Product Development Team shall have been involved in at least two software development projects similar in scope to the Bidder's proposed solution. 2. Each member of the Product Development Team shall have been involved in at least one agile software development project. 3. Each member of the Product Development Team shall have at least 2 years experience in at least one of the following, and between all team members each of the following must be covered. <ul style="list-style-type: none"> a. COBOL and Assembly in a CICS mainframe environment b. CICS COBOL API in a SQL DB environment c. IBM Resource Access Control Facility (RACF) d. VB6 e. Secure REST APIs f. Enterprise user authentication tools g. Modern security, monitoring, and logging practices for system administration

		<ul style="list-style-type: none"> h. Modular web application development i. Test-driven development j. Automated unit and integration testing k. Automated acceptance testing l. Continuous build processes and tools m. SQL and SQL optimization n. Load and Performance testing o. Security and system administration p. Modern continuous monitoring tools q. NIST 800-53 controls
--	--	--

STATE ROLES

ROLE	RESPONSIBILITY
Product Owner	The State will provide one Product Owner. The Product Owner is an empowered individual who will interface with the client's stakeholders, synthesize feedback, and make decisions regarding the product's priorities and scope. The Product Owner, working with stakeholder interests, needs, and insight from the product team, will establish the vision and goals for the System API and prioritize user stories to include in sprints and strategize release cycles.
Project Manager	The State will provide one Project Manager. The Project Manager will manage the iteration objectives, work to remove impediments in the organization, help manage relationships and facilitate team continuous improvement, and coordinates solution implementation and delivery with the Scrum Master(s).
Performance Analyst	The State will provide one Performance Analyst. The Performance Analyst will specify and present key performance data and analysis of the product.
Technical Architect	The State will provide one Technical Architect. The Technical Architect will be responsible for translating the requirements into the architecture and describing/managing it through architecture and design artifacts to provide the overall technical vision.

9. PAYMENTS AND INVOICING

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

a. Submission of Invoices

- 1) Payment shall be made after the completion and acceptance for two sprints (i.e. every four weeks). Invoices shall be submitted after completion and acceptance of two sprints. All invoices shall be submitted in triplicate, detailing the labor category hours (incremental hours shall be billed to the nearest 15 or 30 minutes) and dollars and include the following:
 - i. Transmittal with the Agreement number;
 - ii. A certification statement signed by a company official, attesting to the accuracy of the invoice data; and
 - iii. Copies of signed timesheet(s);
- 2) Invoices shall be submitted directly to:

**Office of Systems Integration
Attn: Accounting Office
2525 Natomas Park Drive, Suite 200
Sacramento, CA 95833**

b. Payment Method

Payment to the Contractor will be made on a time and materials basis per the hourly labor classifications set forth in the Contract. The payment amount for each sprint is capped at a total of each resource's labor classification rate multiplied by 90 hours. A sprint is defined as a two (2) week period.

c. Payment Frequency

Payment shall be made after the completion and acceptance for two sprints (i.e. every four weeks).

d. Payment Withhold

To ensure satisfactory performance by the Contractor and mitigate risk to the State, the State will withhold ten percent (10%) from each payment. The State will release the Withhold payment to the Contractor at the conclusion of the entire Contract, provided that all accepted user stories have achieved the Release-level Definition of Done.

10. POINTS OF CONTACT

Contractor – Contract Manager:	
Name, Title:	[To be completed upon agreement award.]
Address:	
Telephone Number:	
Fax Number:	
E-mail address:	

State – Contract Manager:	
Name	Robyn Sasaki
Address:	744 P Street, 12thFloor – OB 9, MS 9-12-83
Telephone Number:	(916) 654-0600
Fax Number:	
E-mail address:	Robyn.Sasaki@osi.ca.gov

11. STATE FURNISHED ITEMS

The following items shall be provided by the State to support this effort:

- a. Office work space for the duration of the Agreement includes desk, chair, desk phone, and Internet connection.
- b. Access to office building and office suite.
- c. All policies and procedures regarding access to and the use of the state facilities are applicable.
- d. Collaboration, version control, and agile project management software services.
- e. Integration, Training, Staging and Production Environments.

12. CONTRACTOR FURNISHED ITEMS

- a. Contractor to provide primary computer workstation (desktop or laptop).
- b. Contractor to provide development and system test environments at no cost to the State.

13. RESPONSIBILITIES OF PARTIES

- a. **Contractor Responsibilities**

- 1) All work products and deliverables shall be stored on the State document repository (e.g. GitHub, Slack) in a format compatible with OSI document standards. The most current version of all work products and deliverables shall be continuously available for State review at all times.
- 2) The Contractor shall receive all project communications and has the authority to act on all aspects of the services. This person will review the Agreement and associated Agreement documents with the State Contract Manager to ensure understanding of the responsibilities of both parties.
- 3) Prior to expiration of the Agreement, the Contractor shall return all State property, including security badges to the State Contract Manager.
- 4) As part of this Agreement, the Contractor (data custodian) shall be responsible for all costs incurred by the State (data owner) due to any and every security incident resulting from the Contractor's failure to perform or negligent acts of its personnel, and resulting in an unauthorized disclosure, release, access, review, or destruction; or loss, theft or misuse of an information asset. If the Contractor experiences an actual or potential loss of data or breach of data security, the Contractor shall, within two (2) hours of its discovery thereof, report the loss or security breach to the OSI Information Security Officer at osiinfosecurity@osi.ca.gov. If the State determines that notice to the individual(s) whose data has been lost or breached is appropriate, the contractor will bear any and all costs associated with the notice or any mitigation selected by the State. These costs include, but are not limited to, consultant time, material costs, postage, media announcements, and other identifiable costs associated with the breach or loss of data.
- 5) The Contractor shall comply with all applicable State policies including, but not limited to (State Administrative Manual 5300-5399, State Information Management Manual procedures, and OSI's security policies including, but not limited to, it's Acceptable Use Policy, Confidentiality and Non-Disclosure Policy, CHHS Security Policies and OSI Security templates, which may be found at www.osi.ca.gov. (See Attachment III-F, Special Provisions.)
- 6) All Contractor-owned or managed laptops, Ultra books, net books, tablets, Smart phones and similar devices, if allowed by the State Contractor Manager, shall be encrypted using commercial third-party encryption software. The encryption software shall meet the level standards of National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules. Additionally, anti-virus, anti-malware software shall be used and kept up to date along with software patches and supported versions. The OSI Information Security Office shall have the right to audit Contractor-owned devices connected to State networks.

- 7) If Contractor use of removable media storage devices (i.e. Universal Serial Bus [USB] thumb drives, disk tapes, micro SD, SD cards, CD/DVD, etc.) is allowed by the State Contract Manager, all electronic files stored on the removable media storage device used to store State information shall be encrypted using a commercial third-party encryption software. The encryption software shall meet the standards set forth in NIST FIPS 140-2. Information stored on approved removable storage devices shall not be copied to any unencrypted computer (i.e., desktop or laptop) not connected to State network. Any personally identifiable information, personal health information, or other confidential information shall be encrypted when stored on State network file shares or document repositories.

b. State Responsibilities

- 1) The State Product Owner will provide product vision, prioritization and User Story acceptance.
- 2) The State Project Director shall receive all project communications and has the authority to act on all aspects of the services. This person will review the Agreement and associated Agreement documents with the Contractor to ensure understanding of the responsibilities of both parties.
- 3) The State will provide timely review and approval of the information and documentation provided in order for the Contractor to perform its obligations under this Agreement.
- 4) The State will provide the following software tools: Slack, Pivotal Tracker, and GitHub.

State of California
Office of Systems Integration

RFP OSI 31326
Statement of Work
December 21, 2015

**ATTACHMENT 1
SPECIAL PROVISIONS**

State of California
Office of Systems Integration

RFP OSI 31326
Statement of Work
December 21, 2015

**ATTACHMENT 2
DEFINITIONS**

State of California
Office of Systems Integration

RFP OSI 31326
Statement of Work
December 21, 2015

ATTACHMENT 3
NIST 800-53 OPERATIONAL

State of California
Office of Systems Integration

RFP OSI 31326
Statement of Work
December 21, 2015

ATTACHMENT 4
NIST 800-53 OPERATIONAL

ATTACHMENT 5
Contractor Sprint Status Report
[Sample]
[Insert page 1 of #]
For [insert reporting period -- month and year]

Contractor:	[Company Name]
Agreement #:	[Project Agreement Number]
Title:	[Project Title]

[This sample template describes the required contents of the Contractor's monthly status report.]

1. Introduction

[A brief overview of the activity completed.]

2. Activity Summary

[This section shall contain the information listed below. Planned user stories and accepted user stories.]

3. Open Impediments.

[Impediments that were not resolved during the sprint.]

4. Technical Debt.

[New accumulated technical debt and resolved technical debt during the sprint.]

ATTACHMENT 6
Contractor Status Report
[Sample]
[Insert page 1 of #]
For [insert reporting period -- month and year]

Deliverables this Month -- *[Show any deliverables that were provided, or should have been provided, during the month. For example, the monthly report for June would probably list the report for May that was delivered in June. Overdue or late deliverables require an explanation.]*

Table 1. Deliverables this Month

DELIVERABLE TITLE	SOW REFERENCE	DATE DUE	DATE DELIVERED
[Deliverable title, from SOW requirement]	[Reference, as used in SOW; i.e., task number or unique reference]	[SOW due date]	[Actual delivery date]

Deliverables Status - *[List all of the deliverables from the SOW, with current status. Each deliverable, whether delivered or due, should be shown. Periodic deliverables do not need to be listed more than once—see example. Other, ad-hoc deliverables should also be listed. These items should also be tied to the SOW paragraph that the tasking fell under.]*

Table 2. Deliverables Status

DELIVERABLE TITLE	SOW REFERENCE	DATE DUE	DATE DELIVERED
[Deliverable title, from SOW requirement]	[Reference, as used in SOW; i.e., task number, or unique reference]	[SOW due date]	[Actual delivery date]
Monthly Report	[Example: Task 1.2 – Status Report]	Monthly	Monthly

Concerns/Issues -- *[List any concerns or issues that are pertinent to completion of the SOW tasks. If there are no concerns or issues, please indicate by a statement such as “None at this time.”]*

Financial Summary -- *[Show the task’s costs vs. the expenditure plan as presented in the TAP. If no TAP was submitted for your tasking, the status should still be shown against anticipated expenditures.]*

[Any significant variance (greater than ten (10) percent, or as stated in the contractor’s SOW) should be explained in the comment column. Variance is defined as “Actual-Budgeted”.]

State of California
Office of Systems Integration

RFP OSI 31326
Statement of Work
December 21, 2015

Signed by Contractor Contract Manager: _____ **Date:** _____

Approved/Signed by State Contract Manager: _____ **Date:** _____



ATTACHMENT 7
ADD, DELETE OR SUBSTITUTE
CONTRACTOR PERSONNEL REQUEST FORM

Contractor Name		Contractor Phone No.	Date	
Project Name/Agreement Number				
Personnel To Be Added	Personnel Replaced	Proposed Effective Date	Classification	Resume Meets MQs and requirements
				<input type="checkbox"/>
Personnel To Be Deleted	Date Effective	Reason		
		Reason:		
Comments/Special Instructions				
<p>Please note: The changes as indicated in this request are being made at no additional cost to the STATE. – Sample (Include this language, if applicable).</p>				
STATE Acceptance		Contractor Acceptance		
Division/Project		Contractor (If other than an individual, state whether a corporation, partnership, etc.)		
By (Authorized Signature)		By (Authorized Signature)		
Printed Name of Person Signing		Printed Name of Person Signing		

State of California
Office of Systems Integration

RFP OSI 31326
Statement of Work
December 21, 2015

Title	Title

ATTACHMENT 8 **OSI SPECIAL PROVISIONS**

Special Provisions shall include any special directions or project specific requirements that are not otherwise stated explicitly in the agreement.

I. OSI SECURITY

Information Confidentiality and Security Requirements for Leveraged Procurements

1. **Definitions.** For purposes of this Exhibit, the following definitions shall apply:
 - a. **Public Information:** Information that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6270) or other applicable state or federal laws.
 - b. **Confidential Information:** Information that is exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6270) or other applicable state or federal laws.
 - c. **Sensitive Information:** Information that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive Information may be either Public Information or Confidential Information. It is information that requires a higher than normal assurance of accuracy and completeness. Thus, the key factor for Sensitive Information is that of integrity. Typically, Sensitive Information includes records of agency financial transactions and regulatory actions.
 - d. **Personal Information:** Information that identifies or describes an individual, including, but not limited to, their name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. **It is OSI's policy to consider all information about individuals private unless such information is determined to be a public record.** This information shall be protected from inappropriate access, use, or disclosure and shall be made accessible to data subjects upon request. Personal Information includes the following:

Notice-triggering Personal Information: Specific items of personal information (name plus Social Security number, driver license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person. For purposes of this provision, identity shall include, but not be limited to name, identifying number,

symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph. See Civil Code sections 1798.29 and 1798.82.

2. **Nondisclosure.** The Contractor and its employees, agents, or subcontractors shall protect from unauthorized disclosure any Personal Information, Sensitive Information, or Confidential Information (hereinafter identified as PSCI).
 3. The Contractor and its employees, agents, or subcontractors shall not use any PSCI for any purpose other than carrying out the Contractor's obligations under this Agreement.
 4. The Contractor and its employees, agents, or subcontractors shall promptly transmit to the OSI State Contract Manager all requests for disclosure of any PSCI not emanating from the person who is the subject of PSCI.
 5. The Contractor shall not disclose, except as otherwise specifically permitted by this Agreement or authorized by the person who is the subject of PSCI, any PSCI to anyone other than OSI without prior written authorization from the OSI State Contract Manager, except if disclosure is required by State or Federal law.
 6. The Contractor shall observe the following requirements:
 - a. **Requirements and Guidelines.**
 - 1) The Contractor shall classify their data pursuant to the California State Administrative Manual (SAM) 5305.5.
 - 2) The Contractor shall comply with the following:
 - i. The California Information Practices Act (Civil Code Sections 1798 et seq.);
 - ii. Security provisions of the SAM (Chapters 5100 and 5300) and the California Statewide Information Management Manual (SIMM) (Sections 58-C, 58-D, 66-B, 5305-A, 5310-A and B, 5325-A and B, 5330-A, B and C, 5340-A, B and C, 5360B);
 - iii. Privacy provisions of the Federal Privacy Act of 1974;
 - 3) The Contractor shall comply with the information security and privacy controls set forth in the National Institute of Standards and Technology (NIST) Special Publication (SP); including but not limited to NIST 800-53R4 (tailored to OSI Requirements for a Low or Moderate Level Of Concern).

- b. **Safeguards.** The Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of personal, sensitive, and confidential information (PSCI), including electronic PSCI that it creates, receives, maintains, uses, or transmits on behalf of OSI. 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 appropriate levels of security (confidentiality, integrity, and availability) for the data based on data categorization and classification and FIPS Publication 199 protection levels, Including at a minimum the following safeguards:

1) **Personnel Controls**

- a) **Employee Training.** All workforce members who assist in the performance of functions or activities on behalf of OSI, or access or disclose OSI Protected Health Information (PHI) or Personally Identifiable Information (PII) shall complete information privacy and security training, at least annually, at the Contractor's expense. Each workforce member who receives information privacy and security training shall sign a certification, indicating the member's name and the date on which the training was completed. These certifications shall be retained for a period of six (6) years following agreement termination.
- b) **Employee Discipline.** Appropriate sanctions shall be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
- c) **Confidentiality Statement.** All persons that will be working with OSI PSCI shall sign a confidentiality statement. The statement shall include at a minimum, General Use, Security and Privacy safeguards, Unacceptable Use, and Enforcement Policies. The statement shall be signed by the workforce member prior to access to OSI PSCI. The statement shall be renewed annually. The Contractor shall retain each person's written confidentiality statement for OSI inspection for a period of three (3) years following agreement termination.
- d) **Background Check.** Before a member of the Contractor's workforce may access OSI PSCI, the Contractor shall conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk to the security or integrity of

confidential data or a risk for theft or misuse of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following agreement termination.

2) Technical Security Controls

- a. **Workstation/Laptop Encryption.** All workstations and laptops that process and/or store OSI PSCI shall be encrypted with an OSI approved solution (i.e. FIPS 140-2). The encryption solution shall be full disk.
- b. **Minimum Necessary.** Only the minimum necessary amount of OSI PSCI may be downloaded to a laptop or hard drive when absolutely necessary for current business purposes.
- c. **Removable Media Devices.** All electronic files that contain PSCI data shall be encrypted when stored on any removable media type device (i.e. USB thumb drives, floppies, CD/DVD, etc.) with an OSI approved solution (i.e. FIPS 140-2).
- d. **Email Security.** All emails that include OSI PSCI shall be sent in an encrypted method using an OSI approved solution.
- e. **Antivirus Software.** All workstations, laptops, other devices, and systems that process and/or store OSI PSCI shall have a commercial third-party anti-virus software solution with a minimum daily automatic update.
- f. **Patch Management.** All workstations, laptops, other devices, and systems that process and/or store OSI PSCI shall have security patches applied and up-to-date.

g. **User IDs and Password Controls.** All users shall be issued a unique user name for accessing OSI PSCI. Passwords shall not to be shared. Passwords shall adhere to the following:

- Be at least eight characters
- Be a non-dictionary word
- Not be stored in readable format on the computer
- Be changed every 90 days
- Be changed if revealed or compromised

Password shall be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation symbols)

- h. **Data Destruction.** The Contractor shall meet the standards as set forth in NIST800-88 for destruction of data. All OSI PSCI shall be wiped from systems when the data is no longer necessary. The wipe method shall conform to Department of Defense standards for data destruction. If data was PII or PHI, then the Gutmann 35 pass wipe is required. All OSI PSCI on removable media shall be returned to OSI when the data is no longer necessary. Once data has been destroyed and logged, the OSI State Contract Manager shall be notified and provided logs for auditing and retention period.
- i. **Remote Access.** Any remote access to OSI PSCI shall be executed over an encrypted method approved by OSI. All remote access shall be limited to minimum necessary and least privilege principles. Remote Access shall meet security standards as defined in SAM 5360.1 and SIMM 5360-A.

3) System Security Controls

- a. **System Timeout.** The System shall provide an automatic timeout after no more than 20 minutes of inactivity.

- b. **Warning Banners.** All Systems containing OSI PSCI shall display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. Users shall be directed to log off the system if they do not agree with these requirements.
- c. **System Logging.** The System shall log successes and failures of user authentication at all layers. The System shall log all system administrator/developer access and changes if the system is processing and/or storing PSCI. The System shall log all user transactions at the database layer if processing and/or storing OSI PSCI.
- d. **Access Controls.** The System shall use role based access controls for all user authentications, enforcing the principle of least privilege.
- e. **Transmission Encryption.** Confidential, sensitive or personal information shall be encrypted in accordance with SAM 5350.1 and SIMM 5305-A. All data transmissions shall be encrypted end-to-end using an OSI approved solution, when transmitting OSI PSCI. See the CHHS Security Policy – Data Encryption at the following link: [CHHSA Security Policy Data Encryption](#)
- f. **Host Based Intrusion Detection.** All systems that are accessible via the Internet or store OSI PSCI shall actively use a comprehensive third-party real-time host based intrusion detection and prevention solution.

4) ***System Security Review***

- a. The Contractor shall obtain independent security risk assessment consultants to meet the SAM 5305.7 and NIST standards (800-30, 800-37, 800-39, and 800-53) as well as OWASP standards including but not limited to the Development and Testing Guidelines for web services. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not:
 - Create a mutual or conflicting interest with the organizations where the assessments are being conducted.
 - Self-assess their work.
 - Act as management or employees of the organizations they are serving.
 - Place themselves in advocacy positions for the organizations acquiring their services.
 - Have an affiliation, either personal or business, with the Contractor or subcontractors working under contract with the OSI.
- b. The OSI shall have approval of the independent risk assessment consultants that will perform the security risk assessments prior to the Contractor hiring the firm.
- c. The independent security risk assessment firm shall have references from comparable State agencies (comparable system complexity as OSI).
- d. The Contractor shall have independent security risk assessment consultants conduct security risk assessments every two years of the OSI Project Systems (e.g. CWS/CMS, CWS-NS, CMIPS II, and SFIS) and Project Support Systems (.e.g. shared drives, web sites, web applications, Clarity, Sharepoint, County Access Data, and SARS).
- e. The Contractor shall have the security risk assessment provide a gap analysis using the latest version of the Low or Moderate Tailored Baseline NIST 800-53 security controls.
- f. The State Project Manager or designee and the OSI ISO shall have full access to the results of the independent risk assessment.

- g. The Contractor shall provide to the OSI a Security Assessment Report created by the independent security assessors as defined in NIST 800-53. This report shall contain, as a minimum, identification and score of risks and provide recommended mitigation solutions.

5) Audit Controls

- a. **Log Reviews.** All systems processing and/or storing OSI PSCI shall have a routine procedure in place to review system logs for unauthorized access.
- b. **Change Control.** All systems processing and/or storing OSI PSCI shall have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

6) Business Continuity / Disaster Recovery Controls

- a. **Emergency Mode Operation Plan.** The Contractor shall establish a documented plan to enable continuation of critical business processes and protection of the security of electronic OSI PSCI in the event of an emergency. An emergency is an interruption of business operations for more than 24 hours.
- b. **Data Backup Plan.** The Contractor shall have established documented procedures to backup OSI PSCI to maintain retrievable exact copies of OSI PSCI. The plan shall include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore OSI PSCI should it be lost. At a minimum, the schedule shall be a weekly full backup and monthly offsite storage of OSI data.

7) Paper Document Controls

- a. **Supervision of Data.** OSI PSCI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, or desk. Unattended means that information is not being observed by an employee authorized to access the information. OSI PSCI 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 OSI PSCI is contained shall be escorted and OSI PSCI shall be kept out of sight while visitors are in the area.

- c. **Confidential Destruction.** The Contractor shall meet the standards as set forth in NIST 800-88 for destruction of data. OSI PSCI shall be disposed of through confidential means, such as cross cut shredding and pulverizing.
- d. **Removal of Data.** OSI PSCI shall not be removed from the premises of the Contractor except with express written permission of OSI.
- e. **Faxing.** Faxes containing OSI PSCI 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. Contractor fax machines shall be located in secure areas, per SAM 5365.1.
- f. **Mailing.** OSI PSCI shall only be mailed using secure methods. Large volume mailings of OSI PSCI shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail shall be encrypted with an OSI approved solution.

8) Physical Transport of Paper/Electronic Data/Media

There are specific precautions that shall be taken when transporting electronic data/media. The data/media shall be wrapped or sealed in an envelope or pouch in such a manner that the contents cannot be identified during the transportation process. The outside of the container shall clearly identify the addressee, which includes the name, address and telephone number where he/she can be reached. Departments should ensure that transported data/media be delivered only to the appropriate individuals who are authorized to receive the information. This can be accomplished by implementing a tracking method by which the sender and the recipient can sign and verify delivery and receipt of the information.

The Contractor shall ensure that there is a tracking process in place for the transportation of data/media, whether in paper records or physical media devices and that accountability is strongly emphasized with the establishment of this process. Existing tracking processes such as those associated with FedEx, UPS and the U.S. Postal Service are permitted, however when sending information on physical media devices via these methods or by similar means, **the information shall be encrypted.**

- c. **California Public Records Act.** The Contractor shall work cooperatively with the State to respond timely and correctly to public records act requests.
- d. **Security Officer.** The Contractor shall designate a Security Officer to oversee its data security program who will be responsible for carrying out its privacy and security programs and for communicating on security matters with OSI.
- e. **Training.** The Contractor shall provide training on its data privacy and security policies, at least annually, at its own expense, to all its employees and volunteers who assist in the performance of functions or activities on behalf of OSI under this Agreement and use or disclose PSCI.
 - 1) The Contractor shall require each employee and volunteer who receives data privacy and security training to sign a certification, indicating the employee's/volunteer's name and the date on which the training was completed.
 - 2) The Contractor shall retain each employee's/volunteer's written certifications for OSI inspection for a period of three years following agreement termination.
- f. **Breaches.**
 - 1) **Discovery and Notification of Breach.** The Contractor shall be responsible for facilitating the security incident process as described in California Civil Code 1798.29(e), California Civil Code 1798.82(f), and SAM 5340, Incident Management. The Contractor shall notify OSI immediately by telephone call plus email or fax upon the discovery of breach of security of PSCI in computerized form if the PSCI was, or is reasonably believed to have been, acquired by an unauthorized person, or within two hours by email of the discovery of any suspected security incident, intrusion or unauthorized use or disclosure of PSCI in violation of this Agreement, this provision, the law, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the OSI Program Contract Manager, the OSI Privacy Officer and the OSI Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PSCI, notification shall be provided by e-mailing the OSI Security Office at osiinfosecurity@osi.ca.gov. The Contractor shall take:
 - a) Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment and
 - b) Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

- 2) **Investigation of Breach.** The Contractor shall immediately investigate such security incident, breach, or unauthorized use or disclosure of PSCI and within twelve (12) to twenty-four (24) hours of the discovery, shall notify the OSI State Contract Manager, the OSI Privacy Officer, and the OSI Information Security Officer of:
 - a) What data elements were involved and the extent of the data involved in the breach;
 - b) A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PSCI;
 - c) A description of where the PSCI is believed to have been improperly transmitted, sent, or utilized;
 - d) A description of the probable causes of the improper use or disclosure; and
 - e) Whether Civil Code sections 1798.29 or 1798.82 or any other federal or state laws requiring individual notifications of breaches are triggered.
 - 3) **Updates on Investigation.** The Contractor shall provide regular (every 24 hours) updates on the progress of the investigation to the OSI State Contract Manager, the OSI Privacy Officer, and the OSI Information Security Officer.
 - 4) **Written Report.** The Contractor shall provide a written report of the investigation to the OSI Program Contract Manager, the OSI Privacy Officer, and the OSI Information Security Officer within seven (7) working days of the discovery of the breach or unauthorized use or disclosure. The report will, at a minimum, follow the format of SIMM 5340-B. The report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.
 - 5) **Notification of Individuals.** The Contractor shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The OSI State Contract Manager, the OSI Privacy Officer, and the OSI Information Security Officer shall approve the time, manner and content of any such notifications.
7. **Affect on lower tier transactions.** The terms of this Exhibit shall apply to all agreements, subcontracts, and subawards, regardless of whether they are for the

acquisition of services, goods, or commodities. The Contractor shall incorporate the contents of this Exhibit into each subcontract or subaward to its agents, subcontractors, or independent consultants.

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

OSI State Contract Manager	OSI Privacy Officer	OSI Information Security Officer
See the agreement for State Contract Manager information	Privacy Officer c/o OSI Legal Division Office of Systems Integration 2525 Natomas Park Drive, Suite 200 Sacramento, CA 95833 Email: @osi.ca.gov Telephone: (916) 263-0737	Information Security Officer OSI Information Security Office Office of Systems Integration 2525 Natomas Park Drive, Suite 200 Sacramento, CA 95833 Email: osinfosecurity@osi.ca.gov Telephone: (916) 263-0744 or (916) 825-9213

9. **Audits and Inspections.** From time to time, OSI may inspect the facilities, systems, books and records of the Contractor to monitor compliance with the safeguards required in the Information Confidentiality and Security Requirements (ICSR) exhibit. The Contractor shall promptly remedy any violation of any provision of this ICSR exhibit. The fact that OSI inspects, or fails to inspect, or has the right to inspect the Contractor's facilities, systems and procedures does not relieve the Contractor of its responsibility to comply with this ICSR exhibit.

STATEMENT OF WORK - ATTACHMENT II

Acceptance, Accepted	Notice from the State to the Contractor that a Deliverable or service has satisfied the Acceptance Criteria for that Deliverable or service.
Acceptance Criteria	The conditions that must be met before the State Product Owner accepts the particular functionality or User Story. Acceptance criteria may be defined at a system level, a feature level, or a User Story level, but the criteria must be defined before delivery.
Acceptance Test	The functional testing of a module (s), component, or major release of software intended to determine if it meets requirements specified in the Acceptance Criteria. This definition supersedes the definition for Acceptance Tests provided in the CWS-NS General Provisions, paragraph 1. Definitions.
Administration for Children, Youth and Families (ACYF)	The principal operating division of the Department of Health and Human Services. ACYF is the federal sponsor for Child Welfare Services and the Statewide Automated Child Welfare Information Systems (SACWIS) program.
Agile Software Development	An umbrella term for iterative, incremental software development methodologies including Extreme Programming (XP), Scrum, Kanban, Crystal, Dynamic Systems Development Method (DSDM), Lean, and Feature-Driven Development (FDD). Agile development is an alternative to traditional phase-driven "Waterfall" development method, which emphasizes top-down project management, "big design up front," silos for architecture and design, coding, and testing, and extensive documentation. Agile methodologies share an emphasis on small teams delivering small increments of working software with great frequency while working in close collaboration with the customer and adapting to changing requirements.
Agile Sprint Planning	The process by which increments of work are planned, estimated, and committed to by the Contractor.
Allegation	A report provided to law enforcement or a child welfare agencies that describes Child Abuse.
Application Program Interface (API) Assessing	A software intermediary that makes it possible for application programs to interact with each other and share data. An API is often an implementation of REST that exposes a specific software functionality while protecting the rest of the application.
Assessment	The use of historical and current information about the family and the child to determine if the child is safe in their currently living environment. When assessing safety and risk a child welfare worker identifies risk factors and/or appropriate services to improve the family's situation.
Asynchronous JavaScript and XML (AJAX)	A method of building interactive applications for the Web that process user requests without reloading the page.
Business Days	Calendar Days less weekends and State holidays
Calendar Days	All days in a month including weekends and holidays.
Case	A client record for a child or non-minor dependent receiving court ordered or voluntary services.
Child Abuse	See Child Abuse definition in California Welfare and Institutions Code section 300 and California Penal Code sections 11164 -11165.6.
Child Welfare (CW)	Child Welfare staff employed by the State, counties (Child Welfare and Probation) or tribes to provide a full range of necessary services to a child or family.
Worker/staff	
Child Welfare Agency	A county child welfare agency, probation agency or approved Title IV-E tribe that provides services directed toward protecting and promoting the welfare of children.
Child Welfare Services	Public social services directed toward protecting and promoting the welfare of children as defined by Welfare and Institutions Code Section 16501(a).
Configuration Management	A process of automating the replication of a server image from a script, using tools such as Chef, Puppet, Salt, and Ansible.
Contact	In person, writing or telephone communications by a social worker or other persons authorized pursuant to regulations or designated to provide services to a child, youth, parent(s), out-of-home care providers or other persons involved in child welfare services.
Containerization	A method of deploying software within a container. A container, in general, is an isolation implementation within a virtualized operating system. Specific implementations of containerization include Docker, LXC, Rkt, and Warden.
Cross-Reporting	The process by which child welfare agencies and law enforcement agencies are required to notify each other when a report of child abuse, neglect, or exploitation is received.
CWS-NS General Provisions	CWS-NS General Provisions refers to the CWS-NS General Provisions - Information Technology document.
Deficiencies	A failure of a Deliverable or service, or an omission, defect, error, or inadequacy in a Deliverable or service, causing it not to conform to applicable specifications.
Definition of Done	The Acceptance Criteria by which a unit of work (e.g User Story, release) is assessed to determine completeness and ensure quality standards are applied prior to acceptance.
Design Spike	A design approach whose purpose is to provide the answer or solution that previously could not be estimated until the development team conducted actual work to resolve a design problem.
Developments	Materials, including but not limited to, designs, drawings, technical data or design documents, reports, memoranda, studies, plans, formulas, compositions, processes, specifications, notes, statements, artwork, techniques, Software (including data and related documentation), exhibits, and any other documents or materials that are: (i) made, conceived of, or developed, in whole or in part, by the Contractor or its subcontractors in its performance of services; or (ii) modifications made by or on behalf of the Contractor to Contractor Technology (but not Contractor Technology itself)
Differential Response (DR)	An approach that allows child protective services to respond differently to accepted reports of child abuse and neglect. Differential Response services are provided by community-based organizations and can either be provided to the family in lieu of Child Welfare Services (Path 1) or as a supplement to Child Welfare Services (Path 2). A Path 1, Differential Response is chosen when allegations do not meet statutory definitions of abuse or neglect, and the family is given an opportunity to embrace community services. A Path 2 Differential Response is chosen when reports meet statutory definitions of abuse or neglect, and assessments indicate that with targeted services a family is likely to make needed improvements to improve child safety.
Disposition	The resolution or outcome of a child abuse investigation. In child welfare, there are three identified outcomes: substantiated, inconclusive or unfounded.
Documentation	Both external to the Product and internal to the Product materials for both the process and Product and includes printed materials (e.g., quick start cards, manuals and books), computer-readable text (e.g., plain text files, hyperlinked help systems and web pages), audio and video (e.g., computer-based video files, video tapes and telephone-based question and answer service) and built-in documentation (e.g., built-in manuals and source code comments). This definition supersedes the definition for Documentation provided in the CWS-NS General Provisions, paragraph 1. Definitions.
Feature Impediment	A collection of User Stories or requirements of similar nature that together fulfill a stakeholder need. Anything that keeps the team from getting work done and that slows velocity.

Intake	The initial entry point into child welfare services that include processes to receive child abuse, neglect or exploitation referrals from community members and mandated reporters.
Intake Module	Refers to the Intake and Investigations functionality.
Intake Worker	A child welfare worker who receives, records, screens and assesses reports to determine whether a reported incident of abuse, neglect, or exploitation requires a response and what type.
Integration Test	
Interoperability	The phase in software testing in which individual software modules are combined and tested as a group.
Investigation	The seamless implementation and integration of the various components of each module and across all modules that together form the CWS-NS. The process CWS workers utilize to collect information through in-person contacts with the child and family, and contacts with individuals who may have information about the events related to allegations in a referral. The caseworker assesses safety and risk with both the child and family to determine if the child is safe in their current living environment, to identify risk factors and/or to identify appropriate services that may improve the family's situation.
Investigator	A licensing worker with peace officer status who investigates the most serious complaint allegations made against a licensee or foster parent, and a county worker who investigates complaints against a foster parent.
Joyful	In the context of user interface (UI), a joyful UI is a natural user interface that feels intuitive to use and focuses on the joy of doing versus accomplishment and task completion.
Key Staff	Contractor staff positions designated by the State in the Statement of Work that are essential to the Project.
Legacy System	An old method, technology, computer system, or application program, or, relating to, or being a previous or outdated computer system. In this contract the Legacy System refers to the Child Welfare Services/Case Management System (CWS/CMS).
Mandated Reporter	
Module	A person employed in a profession designated within the Child Abuse and Neglect Reporting Act (California Penal Code sections 11164 - 11174.3) who is legally obligated to report to law enforcement and/or child welfare services any incident "reasonably suspected" of being child abuse or neglect.
Office of Systems Integration (OSI)	The packaged collection of software created pursuant to this Contract in order to fulfill the scope of work.
Open Source Software	The State entity which contracts with the CWS-NS Services Contractor on behalf of the State.
Parties or Party	Software where source code is made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose
Pattern Library	Refers to the contracting entities, Contractor and OSI, collectively and in the singular.
Performance Standards	A collection of user interface design patterns.
Perpetrator	The standards relating to the operation of an individual Module and/or the System as a whole as described in the Contract.
Product (or Program Product)	A person who is believed to commit an act of child abuse.
Product Backlog	The packaged collection of software created pursuant to this Contract in order to fulfill the scope of work. This definition supersedes the definition for Program Product provided in the CWS-NS General Provisions, paragraph 1. Definitions.
Product Owner	A prioritized and estimated list of all outstanding product/project requirements, features, defects and other work items.
Product Roadmap	An empowered individual who will interface with the client's stakeholders, synthesize feedback, and make decisions on the product's priorities and scope.
Project	The high-level initiatives and the planned steps that communicate direction and progress to internal teams and external stakeholders.
Project Director	The planned undertaking regarding the entire subject matter, the terms of the Contract, and the activities of the parties related to the Child Welfare Services New System.
Proposal	The individual chosen by OSI to manage the Project and given the responsibilities of the day-to-day management for the Project.
Referral to community agency	The document submitted by the Contractor in response to the procurement document for this Contract.
Referrals	When the determination that a child abuse investigation is not warranted but other needs are identified, the referral may be sent to a community agency for follow-up.
Reporting Party	Emergency response Referrals contain information in regard to allegations of child abuse, neglect, or exploitation as defined by Penal Code Section 11165 et seq., Welfare and Institutions Code, and the Division 31 regulations. Emergency response referrals do not include inappropriate inquiries such as those regarding aid payments, Medi-Cal cards, etc.
REST	A person who reports to child welfare services any incident "reasonably suspected" of being child abuse or neglect.
RESTful	A coordinated set of constraints to the design of components in a distributed hypermedia system that can lead to a higher-performing and more maintainable architecture.
Risk	A common software architectural style for development of web services.
Safety	The likelihood that a family will abuse or neglect a child in the future.
Screening	The determination as to whether there are present dangers and/or imminent threats of serious harm/maltreatment to a child or children.
Server image	The process used by the Child Welfare Agency to determine whether information received meets criteria for some type of intervention.
Service Manager(s)	A copy of a server state, including the configuration, dependencies, data, software, etc.
Sprint	An empowered individual who will interface with the client's stakeholders, synthesize feedback, and make decisions on the product's priorities and scope.
Strangler Pattern	A regular, repeatable time-boxed work cycle during which work is completed and made ready for review.
Suspected Child Abuse Report (SCAR)	An application development approach to the replacement of legacy systems in which a new application is created around the old application thereby reducing the cost and risk over an approach of a complete rewrite of the system. Slowly, over time, the new application will do more and more of the work and eventually strangle the old legacy application.
Unit Test	A California Department of Justice standard form for Mandated Reporters reporting child abuse.
User Story	An automated piece of code that invokes a unit of work in the system and then checks a single assumption about the behavior of that unit of work.
User Story Approval	A tool used in Agile software development to capture a description of a software feature from an end-user perspective. The user story describes the type of user, what they want and why. A user story helps to create a simplified description of a requirement and contains acceptance criteria.
UX/UI Design	The process by which the State Product Owner approves the work completed for each User Story by verifying that the Contractor has met the Definition of Done.
Victim	UX Design refers to the term User Experience Design, while UI Design stands for User Interface Design. Both elements are crucial to a product and work closely together. Where UX Design is a more analytical and technical field, UI Design is closer to what we refer to as graphic design, though the responsibilities are somewhat more complex.
	A child that has been alleged to or has suffered neglect, physical abuse, psychological or emotional abuse, sexual abuse, or exploitation.

CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY

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

CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY

- cc) "**Operating Software**" means those routines, whether or not identified as Program Products, that reside in the Equipment and are required for the Equipment to perform its intended function(s), and which interface the operator, other Contractor-supplied programs, and user programs to the Equipment.
- dd) "**Operational Use Time**" means for performance measurement purposes, that time during which Equipment is in actual operation by the State. For maintenance Operational Use Time purposes, that time during which Equipment is in actual operation and is not synonymous with power on time.
- ee) "**Period of Maintenance Coverage**" means the period of time, as selected by the State, during which maintenance services are provided by the Contractor for a fixed monthly charge, as opposed to an hourly charge for services rendered. The Period of Maintenance Coverage consists of the Principal Period of Maintenance and any additional hours of coverage per day, and/or increased coverage for weekends and holidays.
- ff) "**Preventive Maintenance**" means that maintenance, performed on a scheduled basis by the Contractor, which is designed to keep the Equipment in proper operating condition.
- gg) "**Principal Period of Maintenance**" means any nine consecutive hours per day (usually between the hours of 7:00 a.m. and 6:00 p.m.) as selected by the State, including an official meal period not to exceed one hour, Monday through Friday, excluding holidays observed at the installation.
- hh) "**Programming Aids**" means Contractor-supplied programs and routines executable on the Contractor's Equipment which assists a programmer in the development of applications including language processors, sorts, communications modules, data base management systems, and utility routines, (tape-to-disk routines, disk-to-print routines, etc.).
- ii) "**Program Product**" means programs, routines, subroutines, and related items which are proprietary to the Contractor and which are licensed to the State for its use, usually on the basis of separately stated charges and appropriate contractual provisions.
- jj) "**Remedial Maintenance**" means that maintenance performed by the Contractor which results from Equipment (including Operating Software) failure, and which is performed as required, i.e., on an unscheduled basis.
- kk) "**Software**" means an all-inclusive term which refers to any computer programs, routines, or subroutines supplied by the Contractor, including Operating Software, Programming Aids, Application Programs, and Program Products.
- ll) "**Software Failure**" means a malfunction in the Contractor-supplied Software, other than Operating Software, which prevents the accomplishment of work, even though the Equipment (including its Operating Software) may still be capable of operating properly. For Operating Software failure, see definition of Equipment Failure.
- mm) "**State**" means the government of the State of California, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the State of California.
- nn) "**System**" means the complete collection of Hardware, Software and services as described in this Contract, integrated and functioning together, and performing in accordance with this Contract.
- oo) "**U.S. Intellectual Property Rights**" means intellectual property rights enforceable in the United States of America, including without limitation rights in trade secrets, copyrights, and U.S. patents.

2. CONTRACT FORMATION:

- a) If this Contract results from a sealed bid offered in response to a solicitation conducted pursuant to Chapters 2 (commencing with Section 10290), 3 (commencing with Section 12100), and 3.6 (commencing with Section 12125) of Part 2 of Division 2 of the Public Contract Code (PCC), then Contractor's bid is a firm offer to the State which is accepted by the issuance of this Contract and no further action is required by either party.
- b) If this Contract results from a solicitation other than described in paragraph a), above, the Contractor's quotation or proposal is deemed a firm offer and this Contract document is the State's acceptance of that offer.
- c) If this Contract resulted from a joint bid, it shall be deemed one indivisible Contract. Each such joint Contractor will be jointly and severally liable for the performance of the entire Contract. The State assumes no responsibility or obligation for the division of orders or purchases among joint Contractors.
- 3. **COMPLETE INTEGRATION:** This Contract, including any documents incorporated herein by express reference, is intended to be a complete integration and there are no prior or contemporaneous different or additional agreements pertaining to the subject matter of the Contract.
- 4. **SEVERABILITY:** The Contractor and the State agree that if any provision of this Contract is found to be illegal or unenforceable, such term or provision shall be deemed stricken and the remainder of the Contract shall remain in full force and effect. Either party having knowledge of such term or provision shall promptly inform the other of the presumed non-applicability of such provision.
- 5. **INDEPENDENT CONTRACTOR:** Contractor and the agents and employees of the Contractor, in the performance of this Contract, shall act in an independent capacity and not as officers or employees or agents of the State.
- 6. **APPLICABLE LAW:** This Contract shall be governed by and shall be interpreted in accordance with the laws of the State of California; venue of any action brought with regard to this Contract shall be in Sacramento County, Sacramento, California. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Contract.
- 7. **COMPLIANCE WITH STATUTES AND REGULATIONS:**
 - a) The State and the Contractor warrants and certifies that in the performance of this Contract, it will comply with all applicable statutes, rules, regulations and orders of the United States and the State of California. The Contractor agrees to indemnify the State against any loss, cost, damage or liability by reason of the Contractor's violation of this provision.
 - b) The State will notify the Contractor of any such claim in writing and tender the defense thereof within a reasonable time; and
 - c) The Contractor will have sole control of the defense of any action on such claim and all negotiations for its settlement or compromise; provided that (i) when substantial principles of government or public law are involved, when litigation might create precedent affecting future State operations or liability, or when involvement of the State is otherwise mandated by law, the State may participate in such action at its own expense with respect to attorneys' fees and costs (but not liability); (ii) where a settlement would impose liability on the State, affect principles of California government or public law, or impact the authority of the State, the Department of General Services will have the right to approve or disapprove any settlement or compromise, which approval will not unreasonably be withheld or delayed; and (iii) the State will reasonably cooperate in the defense and in any related settlement negotiations.
 - d) If this Contract is in excess of \$554,000, it is subject to the requirements of the World Trade Organization (WTO) Government Procurement Agreement (GPA).
 - e) To the extent that this Contract falls within the scope of Government Code Section 11135, the Contractor hereby agrees to respond to and resolve any complaint brought to

CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY

- its attention, regarding accessibility of its products or services.
- 8. CONTRACTOR'S POWER AND AUTHORITY:** The Contractor warrants that it has full power and authority to grant the rights herein granted and will hold the State harmless from and against any loss, cost, liability, and expense (including reasonable attorney fees) arising out of any breach of this warranty. Further, the Contractor avers that it will not enter into any arrangement with any third party which might abridge any rights of the State under this Contract.
- a) The State will notify the Contractor of any such claim in writing and tender the defense thereof within a reasonable time; and
 - b) The Contractor will have sole control of the defense of any action on such claim and all negotiations for its settlement or compromise; provided that (i) when substantial principles of government or public law are involved, when litigation might create precedent affecting future State operations or liability, or when involvement of the State is otherwise mandated by law, the State may participate in such action at its own expense with respect to attorneys' fees and costs (but not liability); (ii) where a settlement would impose liability on the State, affect principles of California government or public law, or impact the authority of the State, the Department of General Services will have the right to approve or disapprove any settlement or compromise, which approval will not unreasonably be withheld or delayed; and (iii) the State will reasonably cooperate in the defense and in any related settlement negotiations.
- 9. ASSIGNMENT:** This Contract shall not be assignable by the Contractor in whole or in part without the written consent of the State. The State's consent shall not be unreasonably withheld or delayed. For the purpose of this paragraph, the State will not unreasonably prohibit the Contractor from freely assigning its right to payment, provided that the Contractor remains responsible for its obligations hereunder.
- 10. WAIVER OF RIGHTS:** Any action or inaction by the State or the failure of the State on any occasion, to enforce any right or provision of the Contract, shall not be construed to be a waiver by the State of its rights hereunder and shall not prevent the State from enforcing such provision or right on any future occasion. The rights and remedies of the State herein are cumulative and are in addition to any other rights or remedies that the State may have at law or in equity.
- 11. ORDER OF PRECEDENCE:** In the event of any inconsistency between the articles, attachments, specifications or provisions which constitute this Contract, the following order of precedence shall apply:
- a) These General Provisions – Information Technology (In the instances provided herein where the paragraph begins: "Unless otherwise specified in the Statement of Work" provisions specified in the Statement of Work replacing these paragraphs shall take precedence over the paragraph referenced in these General Provisions);
 - b) Contract form, i.e., Purchase Order STD 65, Standard Agreement STD 213, etc., and any amendments thereto;
 - c) Other Special Provisions;
 - d) Statement of Work, including any specifications incorporated by reference herein;
 - e) Cost worksheets; and
 - f) All other attachments incorporated in the Contract by reference.
- 12. PACKING AND SHIPMENT:**
- a) All Goods are to be packed in suitable containers for protection in shipment and storage, and in accordance with applicable specifications. Each container of a multiple container shipment shall be identified to:
 - i) show the number of the container and the total number of containers in the shipment; and
 - ii) the number of the container in which the packing sheet has been enclosed.
 - b) All shipments by the Contractor or its subcontractors must include packing sheets identifying: the State's Contract number; item number; quantity and unit of measure; part number and description of the Goods shipped; and appropriate evidence of inspection, if required. Goods for different Contracts shall be listed on separate packing sheets.
 - c) Shipments must be made as specified in this Contract, as it may be amended, or otherwise directed in writing by the State's Transportation Management Unit within the Department of General Services, Procurement Division.
- 13. TRANSPORTATION COSTS AND OTHER FEES OR EXPENSES:** No charge for delivery, drayage, express, parcel post, packing, cartage, insurance, license fees, permits, cost of bonds, or for any other purpose will be paid by the State unless expressly included and itemized in the Contract.
- a) The Contractor must strictly follow Contract requirements regarding Free on Board (F.O.B.), freight terms and routing instructions. The State may permit use of an alternate carrier at no additional cost to the State with advance written authorization of the Buyer.
 - b) If "prepay and add" is selected, supporting freight bills are required when over \$50, unless an exact freight charge is approved by the Transportation Management Unit within the Department of General Services Procurement Division and a waiver is granted.
 - c) On "F.O.B. Shipping Point" transactions, should any shipments under the Contract be received by the State in a damaged condition and any related freight loss and damage claims filed against the carrier or carriers be wholly or partially declined by the carrier or carriers with the inference that damage was the result of the act of the shipper such as inadequate packaging or loading or some inherent defect in the Equipment and/or material, the Contractor, on request of the State, shall at Contractor's own expense assist the State in establishing carrier liability by supplying evidence that the Equipment and/or material was properly constructed, manufactured, packaged, and secured to withstand normal transportation conditions.
- 14. DELIVERY:** The Contractor shall strictly adhere to the delivery and completion schedules specified in this Contract. Time, if stated as a number of days, shall mean calendar days unless otherwise specified. The quantities specified herein are the only quantities required. If the Contractor delivers in excess of the quantities specified herein, the State shall not be required to make any payment for the excess Deliverables, and may return them to Contractor at the Contractor's expense or utilize any other rights available to the State at law or in equity.
- 15. SUBSTITUTIONS:** Substitution of Deliverables may not be tendered without advance written consent of the Buyer. The Contractor shall not use any specification in lieu of those contained in the Contract without written consent of the Buyer.
- 16. INSPECTION, ACCEPTANCE AND REJECTION:** Unless otherwise specified in the Statement of Work:
- a) When acquiring Commercial Hardware or Commercial Software, the State shall rely on Contractor's existing quality assurance system as a substitute for State inspection and testing. For all other acquisitions, Contractor and its subcontractors will provide and maintain a quality assurance system acceptable to the State covering Deliverables and services under this Contract and will tender to the State only those Deliverables that have been inspected and found to conform to this Contract's requirements. The Contractor will keep records evidencing inspections and their result, and will make these records available to the State during Contract performance and for three years after final payment. The Contractor shall permit the State to review procedures, practices, processes, and related documents to determine the acceptability of the Contractor's quality assurance System or other similar business practices related to performance of the Contract.

CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY

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

17. SAMPLES:

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

18. WARRANTY:

- a) Unless otherwise specified in the Statement of Work, the warranties in this subsection a) begin upon Acceptance of all Deliverables or services required upon completion of this Contract and end one (1) year thereafter. The Contractor warrants that (i) Deliverables and services furnished hereunder will substantially conform to the requirements of this Contract (including without limitation all descriptions, specifications, and drawings identified in the Statement of Work), and (ii) the Deliverables will be free from material defects in materials and workmanship. Where the parties have agreed to design specifications (such as a Detailed Design Document) and incorporated the same or equivalent in the Statement of Work directly or by reference, the Contractor will warrant that its Deliverables provide all material functionality required thereby. In addition to the other warranties set forth herein, where the Contract calls for delivery of Commercial Software, the Contractor warrants that such Software will perform in accordance with its license and accompanying Documentation. The State's approval of designs or specifications furnished by Contractor shall not relieve the Contractor of its obligations under this warranty.
- b)

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

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

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

21. TERMINATION FOR NON-APPROPRIATION OF FUNDS:

CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY

- a) If the term of this Contract extends into fiscal years subsequent to that in which it is approved, such continuation of the Contract is contingent on the appropriation of funds for such purpose by the Legislature or the federal government. If funds to effect such continued payment are not appropriated, the Contractor agrees to take back any affected Deliverables furnished under this Contract, terminate any services supplied to the State under this Contract, and relieve the State of any further obligation therefor.
- b) In addition to subsection a), payment pursuant to this Contract, whether in whole or in part, is subject to and contingent upon the continuing availability of federal and State funds for the purposes hereof. If such funds, or any part thereof, become unavailable, other than for non-appropriation, as reasonably determined by the State, or if the funds the State relied upon to establish or continue this Contract are withdrawn, reduced, or limited in any way, or if additional or modified conditions are placed on such funding, the State in addition to its other remedies may proceed with any of the following alone or in conjunction:
 - (i) issue a Stop Work order for this Contract or the portion affected thereby;
 - (ii) issue a Work Authorization to the extent the State determines is necessary; or
 - (iii) five (5) days after providing notice, terminate this Contract, in whole or in part, under subsection a) above and make payment to Contractor as provided in subsection a) above as a Termination for Non-Appropriation of Funds.
- c) The State agrees that if it appears likely that subsection a) above will be invoked, the State and Contractor shall agree to take all reasonable steps to prioritize work and Deliverables and minimize the incurrence of costs prior to the expiration of funding for this Contract.
- d) THE STATE AGREES THAT IF PARAGRAPH a) ABOVE IS INVOKED, COMMERCIAL HARDWARE AND SOFTWARE THAT HAS NOT BEEN PAID FOR SHALL BE RETURNED TO THE CONTRACTOR IN SUBSTANTIALLY THE SAME CONDITION IN WHICH DELIVERED TO THE STATE, SUBJECT TO NORMAL WEAR AND TEAR. THE STATE FURTHER AGREES TO PAY FOR PACKING, CRATING, TRANSPORTATION TO THE CONTRACTOR'S NEAREST FACILITY AND FOR REIMBURSEMENT TO THE CONTRACTOR FOR EXPENSES INCURRED FOR THEIR ASSISTANCE IN SUCH PACKING AND CRATING.

22. TERMINATION FOR THE CONVENIENCE OF THE STATE:

- a) The State may terminate performance of work under this Contract for its convenience in whole or, from time to time, in part, if the Department of General Services, Deputy Director Procurement Division, or designee, determines that a termination is in the State's interest. The Department of General Services, Deputy Director, Procurement Division, or designee, shall terminate by delivering to the Contractor a Notice of Termination specifying the extent of termination and the effective date thereof.
- b) After receipt of a Notice of Termination, and except as directed by the State, the Contractor shall immediately proceed with the following obligations, as applicable, regardless of any delay in determining or adjusting any amounts due under this clause. The Contractor shall:
 - (i) Stop work as specified in the Notice of Termination.
 - (ii) Place no further subcontracts for materials, services, or facilities, except as necessary to complete the continuing portion of the Contract.
 - (iii) Terminate all subcontracts to the extent they relate to the work terminated.
 - (iv) Settle all outstanding liabilities and termination settlement proposals arising from the termination of subcontracts;
- c) After termination, the Contractor shall submit a final termination settlement proposal to the State in the form and with the information prescribed by the State. The Contractor shall submit the proposal promptly, but no later than 90 days after the effective date of termination, unless a different time is provided in the Statement of Work or in the Notice of Termination.
- d) The Contractor and the State may agree upon the whole or

any part of the amount to be paid as requested under subsection (c) above.

- e) Unless otherwise set forth in the Statement of Work, if the Contractor and the State fail to agree on the amount to be paid because of the termination for convenience, the State will pay the Contractor the following amounts; provided that in no event will total payments exceed the amount payable to the Contractor if the Contract had been fully performed:
 - (i) The Contract price for Deliverables or services accepted or retained by the State and not previously paid for, adjusted for any savings on freight and other charges; and
 - (ii) The total of:
 - A) The reasonable costs incurred in the performance of the work terminated, including initial costs and preparatory expenses allocable thereto,

CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY

- but excluding any cost attributable to Deliverables or services paid or to be paid;
- B) The reasonable cost of settling and paying termination settlement proposals under terminated subcontracts that are properly chargeable to the terminated portion of the Contract; and
 - C) Reasonable storage, transportation, demobilization, unamortized overhead and capital costs, and other costs reasonably incurred by the Contractor in winding down and terminating its work.
- f) The Contractor will use generally accepted accounting principles, or accounting principles otherwise agreed to in writing by the parties, and sound business practices in determining all costs claimed, agreed to, or determined under this clause.

23. TERMINATION FOR DEFAULT:

- a) The State may, subject to the clause titled "Force Majeure" and to sub-section d) below, by written notice of default to the Contractor, terminate this Contract in whole or in part if the Contractor fails to:
 - i) Deliver the Deliverables or perform the services within the time specified in the Contract or any amendment thereto;
 - ii) Make progress, so that the lack of progress endangers performance of this Contract; or
 - iii) Perform any of the other provisions of this Contract.
- b) The State's right to terminate this Contract under sub-section a) above, may be exercised only if the failure constitutes a material breach of this Contract and if the Contractor does not cure such failure within the time frame stated in the State's cure notice, which in no event will be less than five (5) days, unless the Statement of Work calls for a different period.
- c) If the State terminates this Contract in whole or in part pursuant to this Section, it may acquire, under terms and in the manner the Buyer considers appropriate, Deliverables or services similar to those terminated, and the Contractor will be liable to the State for any excess costs for those Deliverables and services, including without limitation costs third party vendors charge for Manufacturing Materials (but subject to the clause entitled "Limitation of Liability"). However, the Contractor shall continue the work not terminated.
- d) If the Contract is terminated for default, the State may require the Contractor to transfer title, or in the case of licensed Software, license, and deliver to the State, as directed by the Buyer, any:
 - (i) completed Deliverables,
 - (ii) partially completed Deliverables, and,
 - (iii) subject to provisions of sub-section e) below, Manufacturing Materials related to the terminated portion of this Contract. Nothing in this sub-section d) will be construed to grant the State rights to Deliverables that it would not have received had this Contract been fully performed. Upon direction of the Buyer, the Contractor shall also protect and preserve property in its possession in which the State has an interest.
- e) The State shall pay Contract price for completed Deliverables delivered and accepted and items the State requires the Contractor to transfer under section (d) above. Unless the Statement of Work calls for different procedures or requires no-charge delivery of materials, the Contractor and Buyer shall attempt to agree on the amount of payment for Manufacturing Materials and other materials delivered and accepted by the State for the protection and preservation of the property; provided that where the Contractor has billed the State for any such materials, no additional charge will apply. Failure to agree will constitute a dispute under the Disputes clause. The State may withhold from these amounts any sum it determines to be necessary to protect the State against loss because of outstanding liens or claims of former lien holders.

CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY

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

CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY

- accordance with the provisions of the California Prompt Payment Act, Government Code Section 927 et. seq. Unless expressly exempted by statute, the Act requires State agencies to pay properly submitted, undisputed invoices not more than 45 days after (i) the date of acceptance of Deliverables or performance of services; or (ii) receipt of an undisputed invoice, whichever is later.
- 31. TAXES:** Unless otherwise required by law, the State of California is exempt from Federal excise taxes. The State will only pay for any State or local sales or use taxes on the services rendered or Goods supplied to the State pursuant to this Contract.
- 32. NEWLY MANUFACTURED GOODS:** All Goods furnished under this Contract shall be newly manufactured Goods or certified as new and warranted as new by the manufacturer; used or reconditioned Goods are prohibited, unless otherwise specified.
- 33. CONTRACT MODIFICATION:** No amendment or variation of the terms of this Contract shall be valid unless made in writing, signed by the parties and approved as required. No oral understanding or agreement not incorporated in the Contract is binding on any of the parties.
- 34. CONFIDENTIALITY OF DATA:** All financial, statistical, personal, technical and other data and information relating to the State's operation which are designated confidential by the State and made available to the Contractor in order to carry out this Contract, or which become available to the Contractor in carrying out this Contract, shall be protected by the Contractor from unauthorized use and disclosure through the observance of the same or more effective procedural requirements as are applicable to the State. The identification of all such confidential data and information as well as the State's procedural requirements for protection of such data and information from unauthorized use and disclosure shall be provided by the State in writing to the Contractor. If the methods and procedures employed by the Contractor for the protection of the Contractor's data and information are deemed by the State to be adequate for the protection of the State's confidential information, such methods and procedures may be used, with the written consent of the State, to carry out the intent of this paragraph. The Contractor shall not be required under the provisions of this paragraph to keep confidential any data or information which is or becomes publicly available, is already rightfully in the Contractor's possession without obligation of confidentiality, is independently developed by the Contractor outside the scope of this Contract, or is rightfully obtained from third parties.
- 35. NEWS RELEASES:** Unless otherwise exempted, news releases, endorsements, advertising, and social media content pertaining to this Contract shall not be made without prior written approval of the Department of General Services.
- 36. DOCUMENTATION:**
- a) The Contractor agrees to provide to the State, at no charge, all Documentation as described within the Statement of Work, and updated versions thereof, which are necessary or useful to the State to provide for optimal user experience in its use of the Equipment or Software provided hereunder. The Contractor shall provide such Documentation throughout the term of the Contract on an ongoing and iterative basis. The Contractor agrees to provide additional Documentation at prices not in excess of charges made by the Contractor to its other customers for similar Documentation.
 - b) If the Contractor is unable to perform maintenance or the State desires to perform its own maintenance on Equipment purchased under this Contract then upon written notice by the State the Contractor will provide at Contractor's then current rates and fees adequate and reasonable assistance including relevant Documentation to allow the State to maintain the Equipment based on the Contractor's methodology. The Contractor agrees that the State may reproduce such Documentation for its own use in maintaining the Equipment. If the Contractor is unable to perform maintenance, the Contractor agrees to license any other Contractor that the State may have hired to maintain the Equipment to use the above noted Documentation.
- 37. RIGHTS IN WORK PRODUCT:**
- a) All inventions, discoveries, intellectual property, technical communications and records originated or prepared by the Contractor pursuant to this Contract including papers, reports, charts, computer programs, and other Documentation or improvements thereto, and including the Contractor's administrative communications and records relating to this Contract (collectively, the "Work Product"), shall be the property of the State, with the intention of providing an open-source license chosen by the State. The provisions of this sub-section a) may be revised in a Statement of Work.
 - b) Software and other materials developed or otherwise obtained by or for the Contractor or its affiliates independently of this Contract or applicable purchase order ("Pre-Existing Materials") that are not a functional part of any Deliverable do not constitute Work Product. If the Contractor creates derivative works of Pre-Existing Materials, the elements of such derivative works created pursuant to this Contract constitute Work Product, but other elements do not. Nothing in this Section 37 will be construed to interfere with the Contractor's or its affiliates' ownership of Pre-Existing Materials.
 - c) Notwithstanding anything to the contrary in this Contract, the federal government reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, or otherwise use and to authorize others to use for federal government purposes, any software, modifications, and documentation provided by the Contractor hereunder.
 - d) The ideas, concepts, know-how, or techniques relating to data processing, developed during the course of this Contract by the Contractor or jointly by the Contractor and the State may be used by either party without obligation of notice or accounting.
 - e) This Contract shall not preclude the Contractor from developing materials outside this Contract that are competitive, irrespective of their similarity to materials which might be delivered to the State pursuant to this Contract.
- 38. SOFTWARE LICENSE:** Unless otherwise specified in the Statement of Work, the contractor shall use open source Software wherever possible. All licenses must be expressly listed in the deliverable. Regardless of license(s) used (e.g., MIT, GPL, Creative Commons 0) the license(s) shall be clearly listed in the documentation.
- If an open source license provides implementation guidance, the contractor shall ensure compliance with that guidance. If implementation guidance is not available, the contractor shall attach or include the license within the work itself (e.g. code comments at the beginning of a file or contained in a license file within a software repository).
- If the contractor must use Software that does not have an open source license, the contractor shall request permission from the State, in writing, before utilizing that work in any way in connection with the task order. If approved, all licenses shall be clearly set forth in a conspicuous place when work is delivered to the State.
- a) The State may use the Software in the conduct of its own business, and any division thereof
 - b)

CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY

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

39. PROTECTION OF PROPRIETARY SOFTWARE AND OTHER PROPRIETARY DATA:

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

40. [DELETED]

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

42. [DELETED]

43. PATENT, COPYRIGHT AND TRADE SECRET INDEMNITY:

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

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

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

CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY

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

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

44. DISPUTES:

- a) The parties shall deal in good faith and attempt to resolve potential disputes informally.
- b) Pending the final resolution of any dispute arising under, related to or involving this Contract, Contractor agrees to diligently proceed with the performance of this Contract, including the delivery of Goods or providing of services in accordance with the State's instructions regarding this Contract. Contractor's failure to diligently proceed in accordance with the State's instructions regarding this Contract shall be considered a material breach of this Contract.

c) Any final decision of the State shall be expressly identified as such, shall be in writing, and shall be signed by the management-level designee of the State. If the management-level designee of the State fails to render a final decision within fifteen (15) days after receipt of the Contractor's request for a final decision, it shall be deemed a final decision adverse to the Contractor's contentions. The State's final decision shall be conclusive and binding regarding the dispute unless the Contractor commences an action in a court of competent jurisdiction, or with the Victims Compensation Government Claims Board, to contest such decision within 90 days following the date of the final decision or one (1) year following the accrual of the cause of action, whichever is later.

d) e) The date of decision in this section may be modified by mutual consent, as applicable, excepting the time to commence an action in a court of competent jurisdiction.

45. STOP WORK:

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

CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY

- d) The State shall not be liable to the Contractor for loss of profits because of a Stop Work Order issued under this clause.
- 46. EXAMINATION AND AUDIT:** The Contractor agrees that the State or its designated representative shall have the right to review and copy any records and supporting documentation directly pertaining to performance of this Contract. The Contractor agrees to maintain such records for possible audit for a minimum of three (3) years after final payment, unless a longer period of records retention is stipulated. The Contractor agrees to allow the auditor(s) access to such records during normal business hours and in such a manner so as to not interfere unreasonably with normal business activities and to allow interviews of any employees or others who might reasonably have information related to such records. Further, the Contractor agrees to include a similar right of the State to audit records and interview staff in any subcontract related to performance of this Contract. The State shall provide reasonable advance written notice of such audit(s) to the Contractor.
- 47. TIME IS OF THE ESSENCE:**
Time is of the essence in this
Contract.
[DELETED]
- 48. PRIORITY HIRING CONSIDERATIONS:** If this Contract includes services in excess of \$200,000, the Contractor shall give priority consideration in filling vacancies in positions funded by the Contract to qualified recipients of aid under Welfare and Institutions Code Section 11200 in accordance with PCC Section 10353.
- 49. [DELETED]**
- 50. NONDISCRIMINATION CLAUSE:**
- During the performance of this Contract, the Contractor and its subcontractors shall not unlawfully discriminate, harass or allow harassment, against any employee or applicant for employment because of sex, sexual orientation, race, color, ancestry, religious creed, national origin, disability (including HIV and AIDS), medical condition (cancer), age, marital status, and denial of family care leave. The Contractor and subcontractors shall insure that the evaluation and treatment of their employees and applicants for employment are free from such discrimination and harassment. The Contractor and subcontractors shall comply with the provisions of the Fair Employment and Housing Act (Government Code, Section 12990 et seq.) and the applicable regulations promulgated thereunder (California Code of Regulations, Title 2, Section 7285.0 et seq.). The applicable regulations of the Fair Employment and Housing Commission implementing Government Code Section 12990 (a-f), set forth in Chapter 5 of Division 4 of Title 2 of the California Code of Regulations are incorporated into this Contract by reference and made a part hereof as if set forth in full. The Contractor and its subcontractors shall give written notice of their obligations under this clause to labor organizations with which they have a collective bargaining or other agreement.
 - The Contractor shall include the nondiscrimination and compliance provisions of this clause in all subcontracts to perform work under the Contract.
- 51. NATIONAL LABOR RELATIONS BOARD CERTIFICATION:** The Contractor swears under penalty of perjury that no more than one final, unappealable finding of contempt of court by a federal court has been issued against the Contractor within the immediately preceding two-year period because of the Contractor's failure to comply with an order of the National Labor Relations Board. This provision is required by, and shall be construed in accordance with, PCC Section 10296.
- 52. ASSIGNMENT OF ANTITRUST ACTIONS:** Pursuant to Government Code Sections 4552, 4553, and 4554, the following provisions are incorporated herein:
- In submitting a bid to the State, the supplier offers and agrees that if the bid is accepted, it will assign to the State all rights, title, and interest in and to all causes of action it may have under Section 4 of the Clayton Act (15 U.S.C. 15) or under the Cartwright Act (Chapter 2, commencing with Section 16700, of Part 2 of Division 7 of the Business and Professions Code), arising from purchases of Goods, material or other items, or services by the supplier for sale to the State pursuant to the solicitation. Such assignment shall

CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY

- be made and become effective at the time the State tenders final payment to the supplier.
- b) If the State receives, either through judgment or settlement, a monetary recovery for a cause of action assigned under this chapter, the assignor shall be entitled to receive reimbursement for actual legal costs incurred and may, upon demand, recover from the State any portion of the recovery, including treble damages, attributable to overcharges that were paid by the assignor but were not paid by the State as part of the bid price, less the expenses incurred in obtaining that portion of the recovery.
 - c) Upon demand in writing by the assignor, the assignee shall, within one year from such demand, reassign the cause of action assigned under this part if the assignor has been or may have been injured by the violation of law for which the cause of action arose and
 - (i) the assignee has not been injured thereby, or
 - (ii) the assignee declines to file a court action for the cause of action.
- 53. DRUG-FREE WORKPLACE CERTIFICATION:** The Contractor certifies under penalty of perjury under the laws of the State of California that the Contractor will comply with the requirements of the Drug-Free Workplace Act of 1990 (Government Code Section 8350 et seq.) and will provide a drug-free workplace by taking the following actions:
- a) Publish a statement notifying employees that unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance is prohibited and specifying actions to be taken against employees for violations, as required by Government Code Section 8355(a).
 - b) Establish a Drug-Free Awareness Program as required by Government Code Section 8355(b) to inform employees about all of the following:
 - (i) the dangers of drug abuse in the workplace;
 - (ii) the person's or organization's policy of maintaining a drug-free workplace;
 - (iii) any available counseling, rehabilitation and employee assistance programs; and,
 - (iv) penalties that may be imposed upon employees for drug abuse violations.
 - c) Provide, as required by Government Code Section 8355(c), that every employee who works on the proposed or resulting Contract:
 - (i) will receive a copy of the company's drug-free policy statement; and,
 - (ii) will agree to abide by the terms of the company's statement as a condition of employment on the Contract.
- 54. [DELETED]**
- 55. SWEATFREE CODE OF CONDUCT:**
- a) Contractor declares under penalty of perjury that no equipment, materials, or supplies furnished to the State pursuant to the Contract have been produced in whole or in part by sweatshop labor, forced labor, convict labor, indentured labor under penal sanction, abusive forms of child labor or exploitation of children in sweatshop labor, or with the benefit of sweatshop labor, forced labor, convict labor, indentured labor under penal sanction, abusive forms of child labor or exploitation of children in sweatshop labor. The Contractor further declares under penalty of perjury that they adhere to the Sweatfree Code of Conduct as set forth on the California Department of Industrial Relations website located at www.dir.ca.gov, and Public Contract Code Section 6108.
- b) The Contractor agrees to cooperate fully in providing reasonable access to its records, documents, agents or employees, or premises if reasonably required by authorized officials of the State, the Department of Industrial Relations, or the Department of Justice to determine the Contractor's compliance with the requirements under paragraph (a).
- 56. RECYCLED CONTENT REQUIREMENTS:** The Contractor shall certify in writing under penalty of perjury, the minimum, if not exact, percentage of post-consumer material (as defined in the Public Contract Code (PCC) Section 12200-12209), in products, materials, goods, or supplies offered or sold to the State that fall under any of the statutory categories regardless of whether the product meets the requirements of Section 12209. The certification shall be provided by the contractor, even if the product or good contains no postconsumer recycled material, and even if the postconsumer content is unknown. With respect to printer or duplication cartridges that comply with the requirements of Section 12156(e), the certification required by this subdivision shall specify that the cartridges so comply (PCC 12205 (b)(2)). A state agency contracting officer may waive the certification requirements if the percentage of postconsumer material in the products, materials, goods, or supplies can be verified in a written advertisement, including, but not limited to, a product label, a catalog, or a manufacturer or vendor Internet web site. Contractors are to use, to the maximum extent economically feasible in the performance of the contract work, recycled content products (PCC 12203(d)).
- 57. CHILD SUPPORT COMPLIANCE ACT:** For any Contract in excess of \$100,000, the Contractor acknowledges in accordance with PCC Section 7110, that:
- a) The Contractor recognizes the importance of child and family support obligations and shall fully comply with all applicable State and federal laws relating to child and family support enforcement, including, but not limited to, disclosure of information and compliance with earnings assignment orders, as provided in Chapter 8 (commencing with Section 5200) of Part 5 of Division 9 of the Family Code; and
 - b) The Contractor, to the best of its knowledge is fully complying with the earnings assignment orders of all employees and is providing the names of all new employees to the New Hire Registry maintained by the California Employment Development Department.
- 58. AMERICANS WITH DISABILITIES ACT:** The Contractor assures the State that the Contractor complies with the Americans with Disabilities Act of 1990 (42 U.S.C. 12101 et seq.).
- 59. ELECTRONIC WASTE RECYCLING ACT OF 2003:** The Contractor certifies that it complies with the applicable requirements of the Electronic Waste Recycling Act of 2003, Chapter 8.5, Part 3 of Division 30, commencing with Section 42460 of the Public Resources Code. The Contractor shall maintain documentation and provide reasonable access to its records and documents that evidence compliance.
- 60. [DELETED]**
- 61. EXPATRIATE CORPORATIONS:** Contractor hereby declares that it is not an expatriate corporation or subsidiary of an expatriate corporation within the meaning of PCC Sections 10286 and 10286.1, and is eligible to contract with the State.
- 62. DOMESTIC PARTNERS:** For contracts over \$100,000 executed or amended after January 1, 2007, the contractor certifies that the contractor is in compliance with Public Contract Code Section 10295.3.

CWS-NS GENERAL PROVISIONS – INFORMATION TECHNOLOGY

63. SMALL BUSINESS PARTICIPATION AND DVBE PARTICIPATION REPORTING REQUIREMENTS:

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

64. LOSS LEADER:

It is unlawful for any person engaged in business within this state to sell or use any article or product as a "loss leader" as defined in Section 17030 of the Business and Professions Code. (PCC 12104.5(b).).

Statement of Work Attachment 3

NIST 800-53 Operational Security Controls

Baseline Moderate Tailored NIST 800-53r4 Operational Security Controls
Updated: 26 May 2015

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
FAMILY: ACCESS CONTROL		
AC-1	Access Control Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all project personnel: <ul style="list-style-type: none"> 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Access control policy annually; and 2. Access control procedures annually or when major system changes are implemented.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
AC-2	Account Management	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: Information system account types include individual, shared, group, system, emergency, developer/vendor, temporary and service accounts; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by system owner, mission/business owner and chief information security officer for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with provider defined procedures; g. Monitors the use of information system accounts; h. Notifies account managers: <ul style="list-style-type: none"> 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: <ul style="list-style-type: none"> 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements annually; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
AC-2(1)	Account Management	<p><u>AC-2 Control Enhancement:</u></p> <p>(1) ACCOUNT MANAGEMENT / AUTOMATED SYSTEM ACCOUNT MANAGEMENT</p> <p>The organization employs automated mechanisms to support the management of information system accounts.</p>
AC-2(7)	Account Management	<p><u>AC-2 Control Enhancement:</u></p> <p>(7) ACCOUNT MANAGEMENT / ROLE-BASED SCHEMES</p> <p>The organization:</p> <ul style="list-style-type: none"> (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Removes the access privilege(s) upon employees leaving, upon reassignment, and when privileged role assignments are no longer appropriate.
AC-5	Separation of Duties	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Separates duties including, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties.
AC-6	Least Privilege	<p><u>Control:</u> The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
AC-6(1)	Least Privilege	<p><u>AC-6 Control Enhancement:</u></p> <p>(1) <i>LEAST PRIVILEGE / AUTHORIZE ACCESS TO SECURITY FUNCTIONS</i></p> <p>The organization explicitly authorizes access to security functions including, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.</p>
AC-6(2)	Least Privilege	<p><u>AC-6 Control Enhancement:</u></p> <p>(2) <i>LEAST PRIVILEGE / NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS</i></p> <p>The organization requires that users of information system accounts, or roles, with access to security functions including, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists, use non-privileged accounts or roles, when accessing nonsecurity functions.</p>
AC-6(5)	Least Privilege	<p><u>AC-6 Control Enhancement:</u></p> <p>(5) <i>LEAST PRIVILEGE / PRIVILEGED ACCOUNTS</i></p> <p>The organization restricts privileged accounts on the information system to system administrators.</p>
AC-14	Permitted Actions without Identification or Authentication	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Identifies public websites home pages or other public/read-only information that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
AC-17	Remote Access	<u>Control:</u> The organization: <ul style="list-style-type: none"> a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.
AC-17(4)	Remote Access	<u>AC-17 Control Enhancement:</u> <p>(1) <i>REMOTE ACCESS / PRIVILEGED COMMANDS / ACCESS</i></p> The organization: <ul style="list-style-type: none"> a. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for audits and security investigations; and b. Documents the rationale for such access in the security plan for the information system.
AC-18	Wireless Access	<u>Control:</u> The organization: <ul style="list-style-type: none"> a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections.
AC-19	Access Control for Mobile Devices	<u>Control:</u> The organization: <ul style="list-style-type: none"> a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems.
AC-19(5)	Access Control for Mobile Devices	<u>AC-19 Control Enhancement:</u> <p>(5) <i>ACCESS CONTROL FOR MOBILE DEVICES / FULL DEVICE / CONTAINER-BASED ENCRYPTION</i></p> The organization employs full-disk encryption to protect the confidentiality and integrity of information on all mobile devices.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
AC-20	Use of External Information Systems	<p><u>Control:</u> The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:</p> <ul style="list-style-type: none"> a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems.
AC-20(1)	Use of External Information Systems	<p><u>AC-20 Control Enhancement:</u></p> <p>(1) <i>USE OF EXTERNAL INFORMATION SYSTEMS / LIMITS ON AUTHORIZED USE</i></p> <p>The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:</p> <ul style="list-style-type: none"> (a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or (b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.
AC-20(2)	Use of External Information Systems	<p><u>AC-20 Control Enhancement:</u></p> <p>(2) <i>USE OF EXTERNAL INFORMATION SYSTEMS / PORTABLE STORAGE DEVICES</i></p> <p>The organization restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems..</p>
AC-21	Information Sharing	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for release based on business need to know and least privilege; and b. Employs data classification and access controls to assist users in making information sharing/collaboration decisions.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls			
Req #	Title	Requirement	
AC-22	Publicly Accessible Content	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information monthly and removes such information, if discovered. 	
		FAMILY: AWARENESS AND TRAINING	
AT-1	Security Awareness and Training Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all staff, consultants, student assistants, volunteers, contractors, and sub-contractors: <ul style="list-style-type: none"> 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Security awareness and training policy annually; and 2. Security awareness and training procedures annually. 	
AT-2	Security Awareness Training	<p><u>Control:</u> The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):</p> <ul style="list-style-type: none"> a. As part of initial training for new users; b. When required by information system changes; and c. Annually thereafter. 	
AT-2(2)	Security Awareness Training	<p><u>AT-2 Control Enhancement:</u></p> <p>(2) SECURITY AWARENESS / INSIDER THREAT</p> <p>The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.</p>	

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
AT-3	Role-Based Security Training	<p><u>Control:</u> The organization provides role-based security training to personnel with assigned security roles and responsibilities:</p> <ul style="list-style-type: none"> a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. Annually thereafter.
AT-4	Security Training Records	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for three years and HIPAA training for six years.
		FAMILY: AUDIT AND ACCOUNTABILITY
AU-1	Audit and Accountability Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all project personnel: <ul style="list-style-type: none"> 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Audit and accountability policy annually or upon identified need from compliance review; and 2. Audit and accountability procedures annually or upon identified need from compliance review.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
AU-2	Audit Events	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Determines that the information system is capable of auditing the following events: include, but not limited to, password changes, failed logons, failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines that the following events are to be audited within the information system: password changes, failed logons, failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage monthly or when there is an incident that requires investigation.
AU-2(3)	Audit Events	<p><u>AU-2 Control Enhancement:</u></p> <p>(3) AUDIT EVENTS / REVIEWS AND UPDATES</p> <p>The organization reviews and updates the audited events annually.</p>
AU-4	Audit Storage Capacity	<p><u>Control:</u> The organization allocates audit record storage capacity in accordance with a three year retention.</p>
AU-6	Audit Review, Analysis, and Reporting	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Reviews and analyzes information system audit records daily for indications of locked accounts, failed logon attempts, account inactivity, and/or use of administrator privileged account; and b. Reports findings to Chief Technology Officers, Chief Information Officers, and Information Security Officers.
AU-6(1)	Audit Review, Analysis, and Reporting	<p><u>AU-6 Control Enhancement:</u></p> <p>(1) AUDIT REVIEW, ANALYSIS, AND REPORTING / PROCESS INTEGRATION</p> <p>The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
AU-6(3)	Audit Review, Analysis, and Reporting	<p><u>AU-6 Control Enhancement:</u></p> <p>(3) <i>AUDIT REVIEW, ANALYSIS, AND REPORTING / CORRELATE AUDIT REPOSITORIES</i></p> <p>The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.</p>
AU-9(4)	Protection of Audit Information	<p><u>AU-9 Control Enhancement:</u></p> <p>(4) <i>PROTECTION OF AUDIT INFORMATION / ACCESS BY SUBSET OF PRIVILEGED USERS</i></p> <p>The organization authorizes access to management of audit functionality to only information system security officers role.</p>
AU-11	Audit Record Retention	<p><u>Control:</u> The organization retains audit records for three years, or six years for HIPAA to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.</p>
		FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION
CA-1	Security Assessment and Authorization Policies and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all project personnel: <ul style="list-style-type: none"> 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Security assessment and authorization policy annually or upon regulatory changes; and 2. Security assessment and authorization procedures annually or upon regulatory changes and lessons learned from prior security assessments.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
CA-2	Security Assessments	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops a security assessment plan that describes the scope of the assessment including: <ul style="list-style-type: none"> 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation bi-annually or upon major system changes to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to Chief Technology Officers, Chief Information Officers, and Information Security Officers.
CA-2(1)	Security Assessments	<p><u>CA-2 Control Enhancement:</u></p> <p>(1) SECURITY ASSESSMENTS / INDEPENDENT ASSESSORS</p> <p>The organization employs assessors or assessment teams from an independent third party approved by the State organization to conduct security control assessments.</p>
CA-3	System Interconnections	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements annually or upon major system changes.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
CA-3(5)	System Interconnections	<p><u>CA-3 Control Enhancement:</u></p> <p>(5) SYSTEM INTERCONNECTIONS / RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS</p> <p>The organization employs deny-all, permit-by-exception policy for allowing system components to connect to external information systems.</p>
CA-5	Plan of Action and Milestones	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones monthly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
CA-6	Security Authorization	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Assigns a senior-level executive or manager as the authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization annually or when the authorizing official changes.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
CA-7	Continuous Monitoring	<p><u>Control:</u> The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:</p> <ul style="list-style-type: none"> a. Establishment of best practice metrics to be monitored; b. Establishment of weekly for monitoring and monthly for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to Chief Technology Officers, Chief Information Officers, and Information Security Officers at a minimum monthly and immediately upon a new/high/moderate risk being identified (within two hours).
CA-7(1)	Continuous Monitoring	<p><u>CA-7 Control Enhancement:</u></p> <p>(1) CONTINUOUS MONITORING / INDEPENDENT ASSESSMENT</p> <p>The organization employs assessors or assessment teams from an independent third party approved by the State organization to monitor the security controls in the information system at least every two years, or upon significant system/infrastructure changes, or system security breach. To achieve such impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in advocacy positions for the organizations acquiring their services. OSI monitors assessment.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
CA-9	Internal System Connections	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Authorizes internal connections of mobile devices, notebooks, laptop/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.
		FAMILY: CONFIGURATION MANAGEMENT
CM-1	Configuration Management Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all project personnel: <ul style="list-style-type: none"> 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Configuration management policy annually; and 2. Configuration management procedures annually.
CM-2	Baseline Configuration	<p><u>Control:</u> The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.</p>
CM-2(1)	Baseline Configuration	<p><u>CM-2 Control Enhancement:</u></p> <p>(1) <i>BASELINE CONFIGURATION / REVIEWS AND UPDATES</i></p> <p>The organization reviews and updates the baseline configuration of the information system:</p> <ul style="list-style-type: none"> (a) Annually; (b) When required due to system configuration changes; and (c) As an integral part of information system component installations and upgrades.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
CM-2(3)	Baseline Configuration	<p><u>CM-2 Control Enhancement:</u></p> <p>(3) <i>BASELINE CONFIGURATION / RETENTION OF PREVIOUS CONFIGURATIONS</i></p> <p>The organization retains one previous full version to support rollback.</p>
CM-2(7)	Baseline Configuration	<p><u>CM-2 Control Enhancement:</u></p> <p>(7) <i>BASELINE CONFIGURATION / CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS</i></p> <p>The organization:</p> <ul style="list-style-type: none"> a. Mobile devices and laptops will be configured with the strongest security settings and no local admin rights plus removal of unnecessary functions for individuals traveling to locations that the organization deems to be of significant risk; and b. Applies scanning and potentially wiping to the devices when the individuals return.
CM-3	Configuration Change Control	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for the life time of the system plus one year.; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through Configuration Control Boards that convenes at least monthly, or when configuration change activities dictate.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
CM-3(2)	Configuration Change Control	<p><u>CM-3 Control Enhancement:</u></p> <p>(2) <i>CONFIGURATION CHANGE CONTROL / TEST / VALIDATE / DOCUMENT CHANGES</i></p> <p>The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.</p>
CM-4	Security Impact Analysis	<p><u>Control:</u> The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.</p>
CM-4(1)	Security Impact Analysis	<p><u>CM-4 Control Enhancement:</u></p> <p>(1) <i>SECURITY IMPACT ANALYSIS / SEPARATE TEST ENVIRONMENTS</i></p> <p>The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.</p>
CM-5	Access Restrictions for Change	<p><u>Control:</u> The organization defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.</p>
CM-6	Configuration Settings	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Establishes and documents configuration settings for information technology products employed within the information system using security configuration checklists developed by product developers, industry, state and federal agencies that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications based on operational requirements, such as change orders and exemption requests; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
CM-7	Least Functionality	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol), functions, and services on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling.
CM-7(1)	Least Functionality	<p><u>CM-7 Control Enhancement:</u></p> <p>(1) <i>LEAST FUNCTIONALITY / PERIODIC REVIEW</i></p> <p>The organization:</p> <ul style="list-style-type: none"> (a) Reviews the information system annually, when major system changes are implemented, or when an applicable security incident occurs to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and (b) Disables functions, ports, protocols, and services that do not have a validated business need or nonsecure.
CM-7(4) Not Applicable	Least Functionality	<p><u>CM-7 Control Enhancement:</u></p> <p>(4) <i>LEAST FUNCTIONALITY / UNAUTHORIZED SOFTWARE / BLACKLISTING</i></p> <p>The organization:</p> <ul style="list-style-type: none"> (a) Identifies software programs that are not authorized to execute on organizational information systems; (b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and (c) Reviews and updates the list of unauthorized software programs annually or upon major system changes.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
CM-7(5)	Least Functionality	<p><u>CM-7 Control Enhancement:</u></p> <p>(5) <i>LEAST FUNCTIONALITY / AUTHORIZED SOFTWARE / WHITELISTING</i></p> <p>The organization:</p> <ul style="list-style-type: none"> (a) Identifies software programs that are authorized to execute on organizational information systems; (b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and (c) Reviews and updates the list of authorized software programs annually or upon major system changes.
CM-8	Information System Component Inventory	<p><u>Control:</u> The organization:</p> <ol style="list-style-type: none"> a. Develops and documents an inventory of information system components that: <ol style="list-style-type: none"> 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses, manufacturer, device type, model, serial number, and physical location; and 5. Reviews and updates the information system component inventory quarterly.
CM-8(1)	Information System Component Inventory	<p><u>CM-8 Control Enhancement:</u></p> <p>(1) <i>INFORMATION SYSTEM COMPONENT INVENTORY / UPDATES DURING INSTALLATIONS / REMOVALS</i></p> <p>The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
CM-8(3)	Information System Component Inventory	<p><u>CM-8 Control Enhancement:</u></p> <p>(3) <i>INFORMATION SYSTEM COMPONENT INVENTORY / AUTOMATED UNAUTHORIZED COMPONENT DETECTION</i></p> <p>The organization:</p> <ul style="list-style-type: none"> (a) Employs automated mechanisms monthly to detect the presence of unauthorized hardware, software, and firmware components within the information system; and (b) Takes the following actions when unauthorized components are detected: disables component network access and/or isolates the component, and notifies the Chief Technology Officers, Chief Information Officers, and Information Security Officers.
CM-8(4)	Information System Component Inventory	<p><u>CM-8 Control Enhancement:</u></p> <p>(4) <i>INFORMATION SYSTEM COMPONENT INVENTORY / ACCOUNTABILITY INFORMATION</i></p> <p>The organization includes in the information system component inventory information, a means for identifying by position or role, individuals responsible/accountable for administering those components.</p>
CM-8(5)	Information System Component Inventory	<p><u>CM-8 Control Enhancement:</u></p> <p>(5) <i>INFORMATION SYSTEM COMPONENT INVENTORY / NO DUPLICATE ACCOUNTING OF COMPONENTS</i></p> <p>The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.</p>
CM-9	Configuration Management Plan	<p><u>Control:</u> The organization develops, documents, and implements a configuration management plan for the information system that:</p> <ul style="list-style-type: none"> a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places the configuration items under configuration management; and d. Protects the configuration management plan from unauthorized disclosure and modification.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
CM-10	Software Usage Restrictions	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
CM-11	User-Installed Software	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Enforces State Administrative Manual and OSI Standard Software policy governing the installation of software by users; b. Enforces software installation policies through State approved automated tools and Group Policy; and c. Monitors policy compliance at least monthly.
		FAMILY: CONTINGENCY PLANNING
CP-1	Contingency Planning Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all project personnel: <ul style="list-style-type: none"> 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Contingency planning policy annually; and 2. Contingency planning procedures annually.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
CP-2	Contingency Plan	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops a contingency plan for the information system that: <ul style="list-style-type: none"> 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by the Chief Technology Officers, Chief Information Officers, Information Security Officers, Business Continuity Coordinators, Data Owners, and Data Custodians; b. Distributes copies of the contingency plan to personnel based on need-to-know; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system annually or when significant technology and/or business functions change; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to personnel based on need-to-know; and g. Protects the contingency plan from unauthorized disclosure and modification.
CP-2(1)	Contingency Plan	<p><u>CP-2 Control Enhancement:</u></p> <p>(1) CONTINGENCY PLAN / COORDINATE WITH RELATED PLANS</p> <p>The organization coordinates contingency plan development with organizational elements responsible for related plans.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
CP-2(3)	Contingency Plan	<p><u>CP-2 Control Enhancement:</u></p> <p>(3) CONTINGENCY PLAN / RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS</p> <p>The organization plans for the resumption of essential missions and business functions within 48 – 72 hours of contingency plan activation and Recovery Point Object for the data of 1 hour.</p>
CP-2(8)	Contingency Plan	<p><u>CP-2 Control Enhancement:</u></p> <p>(8) CONTINGENCY PLAN / IDENTIFY CRITICAL ASSETS</p> <p>The organization identifies critical information system assets supporting essential missions and business functions.</p>
CP-3	Contingency Training	<p><u>Control:</u> The organization provides contingency training to information system users consistent with assigned roles and responsibilities:</p> <ul style="list-style-type: none"> a. Within one month of assuming a contingency role or responsibility; b. When required by information system changes; and c. Annually thereafter.
CP-4	Contingency Plan Testing	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Tests the contingency plan for the information system annually using project prepared test procedures to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed.
CP-4(1)	Contingency Plan Testing	<p><u>CP-4 Control Enhancement:</u></p> <p>(1) CONTINGENCY PLAN TESTING / COORDINATE WITH RELATED PLANS</p> <p>The organization coordinates contingency plan testing with organizational elements responsible for related plans.</p>
CP-6	Alternate Storage Site	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
CP-6(1)	Alternate Storage Site	<u>CP-6 Control Enhancement:</u> (1) ALTERNATE STORAGE SITE / SEPARATION FROM PRIMARY SITE The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.
CP-6(3)	Alternate Storage Site	<u>CP-6 Control Enhancement:</u> (3) ALTERNATE STORAGE SITE / ACCESSIBILITY The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.
CP-7	Alternate Processing Site	<u>Control:</u> The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of the system (application, network, infrastructure) for essential missions/business functions within 48 – 72 hours and a Recovery Point Objective for the data of 1 hour when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.
CP-7(1)	Alternate Processing Site	<u>CP-7 Control Enhancement:</u> (1) ALTERNATE PROCESSING SITE / SEPARATION FROM PRIMARY SITE The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.
CP-7(2)	Alternate Processing Site	<u>CP-7 Control Enhancement:</u> (2) ALTERNATE PROCESSING SITE / ACCESSIBILITY The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
CP-7(3)	Alternate Processing Site	<p><u>CP-7 Control Enhancement:</u></p> <p>(3) <i>ALTERNATE PROCESSING SITE / PRIORITY OF SERVICE</i></p> <p>The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).</p>
CP-8	Telecommunications Services	<p><u>Control:</u> The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of mission essential services for essential missions and business functions within 48 – 72 hours when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.</p>
CP-8(1)	Telecommunications Services	<p><u>CP-8 Control Enhancement:</u></p> <p>(1) <i>TELECOMMUNICATIONS SERVICES / PRIORITY OF SERVICE PROVISIONS</i></p> <p>The organization:</p> <ul style="list-style-type: none"> (a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and (b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.
CP-8(2)	Telecommunications Services	<p><u>CP-8 Control Enhancement:</u></p> <p>(2) <i>TELECOMMUNICATIONS SERVICES / SINGLE POINTS OF FAILURE</i></p> <p>The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
CP-9	Information System Backup	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Conducts backups of user-level information contained in the information system daily incremental and weekly full; b. Conducts backups of system-level information contained in the information system daily incremental and weekly full; c. Conducts backups of information system documentation including security-related documentation daily incremental and weekly full; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations.
CP-9(1)	Information System Backup	<p><u>CP-9 Control Enhancement:</u></p> <p>(1) <i>INFORMATION SYSTEM BACKUP / TESTING FOR RELIABILITY / INTEGRITY</i></p> <p>The organization tests backup information quarterly to verify media reliability and information integrity.</p>
CP-10	Information System Recovery and Reconstitution	<p><u>Control:</u> The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.</p>
		FAMILY: IDENTIFICATION AND AUTHENTICATION
IA-1	Identification and Authentication Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all project personnel: <ul style="list-style-type: none"> 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Identification and authentication policy annually; and 2. Identification and authentication procedures annually.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
IA-4	Identifier Management	<p><u>Control:</u> The organization manages information system identifiers by:</p> <ul style="list-style-type: none">a. Receiving authorization from the Information Technology Officers and Information Security Officers to assign an individual, group, role, or device identifier;b. Selecting an identifier that identifies an individual, group, role, or device;c. Assigning the identifier to the intended individual, group, role, or device;d. Preventing reuse of identifiers for one year; ande. Disabling the identifier after thirty days of inactivity.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
IA-5	Authenticator Management	<p><u>Control:</u> The organization manages information system authenticators by:</p> <ul style="list-style-type: none"> a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators for individual users, i.e. passwords, every 60 days, authenticators stored within the information system, e.g. password stored in encrypted formats accessible with administrative privileges change, refresh annually, or when a potential security breach of the administrative password has occurred; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.
IA-5(3)	Authenticator Management	<p><u>IA-5 Control Enhancement:</u></p> <p>(1) AUTHENTICATOR MANAGEMENT / IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION</p> <p>The organization requires that the registration process to receive PIV cards, PKI certificates, or hardware based tokens be conducted in person or by a trusted third party before a member of the Information Security Office with authorization by the Information Security Officer.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
IA-8(3)	Identification and Authentication (Non-Organizational Users)	<p><u>IA-8 Control Enhancement:</u></p> <p>(1) <i>IDENTIFICATION AND AUTHENTICATION / USE OF FICAM-APPROVED PRODUCTS</i></p> <p>The organization employs only FICAM-approved information system components in all public facing websites to accept third-party credentials.</p>
		FAMILY: INCIDENT RESPONSE
IR-1	Incident Response Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all project personnel: <ul style="list-style-type: none"> 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Incident response policy annually or upon regulatory changes; and 2. Incident response procedures annually or upon lessons learned from incident responses.
IR-2	Incident Response Training	<p><u>Control:</u> The organization provides incident response training to information system users consistent with assigned roles and responsibilities:</p> <ul style="list-style-type: none"> a. Within 30 days of assuming an incident response role or responsibility; b. When required by information system changes; and c. Annually thereafter.
IR-3	Incident Response Testing	<p><u>Control:</u> The organization tests the incident response capability for the information system annually using approved documented incident response procedures to determine the incident response effectiveness and documents the results.</p>
IR-3(2)	Incident Response Testing	<p><u>IR-3 Control Enhancement:</u></p> <p>(2) <i>INCIDENT RESPONSE TESTING / COORDINATION WITH RELATED PLANS</i></p> <p>The organization coordinates incident response testing with organizational elements responsible for related plans.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
IR-4	Incident Handling	<u>Control:</u> The organization: <ol style="list-style-type: none"> <li data-bbox="616 375 1421 473">a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; <li data-bbox="616 487 1393 585">b. Coordinates incident handling activities with contingency planning activities; and <li data-bbox="616 599 1393 696">c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.
IR-4(1)	Incident Handling	<u>IR-4 Control Enhancement:</u> <p>(1) <i>INCIDENT HANDLING / AUTOMATED INCIDENT HANDLING PROCESSES</i></p> <p>The organization employs automated mechanisms to support the incident handling process.</p>
IR-5	Incident Monitoring	<u>Control:</u> The organization tracks and documents information system security incidents.
IR-6	Incident Reporting	<u>Control:</u> The organization: <ol style="list-style-type: none"> <li data-bbox="616 1072 1421 1170">a. Requires personnel to report suspected security incidents to the organizational incident response capability within two hours of discovery; and <li data-bbox="616 1184 1377 1303">b. Reports security incident information to OSI Contract Manager, OSI Project Director, or the OSI Information Security Officers.
IR-6(1)	Incident Reporting	<u>IR-6 Control Enhancement:</u> <p>(1) <i>INCIDENT REPORTING / AUTOMATED REPORTING</i></p> <p>The organization employs automated mechanisms to assist in the reporting of security incidents.</p>
IR-7	Incident Response Assistance	<u>Control:</u> The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
IR-7(1)	Incident Response Assistance	<p><u>IR-7 Control Enhancement:</u></p> <p>(1) <i>INCIDENT RESPONSE ASSISTANCE / AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT</i></p> <p>The organization employs automated mechanisms to increase the availability of incident response-related information and support.</p>
IR-8	Incident Response Plan	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops an incident response plan that: <ul style="list-style-type: none"> 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by OSI Contract Manager, or OSI Project Director, OSI Chief Technology Officer, OSI Chief Information Officer, and OSI Chief Information Security Officer; b. Distributes copies of the incident response plan to all project personnel; c. Reviews the incident response plan annually or upon regulatory changes and lessons learned; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to all OSI personnel, consultants, and vendors; and f. Protects the incident response plan from unauthorized disclosure and modification.
		FAMILY: MAINTENANCE

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
MA-1	System Maintenance Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to OSI Contract Manager and OSI project librarians: <ul style="list-style-type: none"> 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. System maintenance policy annually or upon regulatory changes; and 2. System maintenance procedures annually or upon regulatory changes and lessons learned.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
MA-2	Controlled Maintenance	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that Information Technology Office, OSI Project Manager, or the OSI Project Operational Manager explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs utilizing a chain of custody process; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes : (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers and State asset tags, if applicable) in organizational maintenance records.
MA-3	Maintenance Tools	<p><u>Control:</u> The organization approves, controls, and monitors information system maintenance tools.</p>
MA-3(1)	Maintenance Tools	<p><u>MA-3 Control Enhancement:</u></p> <p>(1) MAINTENANCE TOOLS / INSPECT TOOLS</p> <p>The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.</p>
MA-3(2)	Maintenance Tools	<p><u>MA-3 Control Enhancement:</u></p> <p>(2) MAINTENANCE TOOLS / INSPECT MEDIA</p> <p>The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
MA-4	Nonlocal Maintenance	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Approves and monitors nonlocal maintenance and diagnostic activities; b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintains records for nonlocal maintenance and diagnostic activities; and e. Terminates session and network connections when nonlocal maintenance is completed.
MA-4(2)	Nonlocal Maintenance	<p><u>MA-4 Control Enhancement:</u></p> <p>(2) <i>NONLOCAL MAINTENANCE / DOCUMENT NONLOCAL MAINTENANCE</i></p> <p>The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.</p>
MA-5	Maintenance Personnel	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
MA-6	Timely Maintenance	<p><u>Control:</u> The organization obtains maintenance support and/or spare parts for all system components within 4 hours for project defined critical components and 24 hours for all other components of failure.</p>
		FAMILY: MEDIA PROTECTION

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
MP-1	Media Protection Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all project personnel: <ul style="list-style-type: none"> 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Media protection policy annually or upon regulatory changes; and 2. Media protection procedures annually or upon regulatory changes and lessons learned.
MP-2	Media Access	<p><u>Control:</u> The organization restricts access to diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks to system administrators or project authorized personnel.</p>
MP-3	Media Marking	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts system administrators from marking as long as the media remain within computer server room.
MP-4	Media Storage	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Physically controls and securely stores Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm within a locked drawer, desk, or cabinet, or a controlled media library; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
MP-5	Media Transport	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Protects and controls Digital media; including, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks; and Non-digital media including, for example, paper; during transport outside of controlled areas using, cryptography, FIPS 140-2 certified algorithm , whether in electronic encrypted media or paper media, a detailed tracking process must be used for media transport; b. Maintains accountability/tracking for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel. e. Data/media wrapped per CHHSA Security Policy – Data Encryption
MP-6	Media Sanitization	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Sanitizes scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices prior to disposal, release out of organizational control, or release for reuse using clearing, purging, cryptographic erase, or destruction in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. c. If the media is staying in OSI possession, NukeBoot with a DoD, seven pass wipe configuration is used prior to reuse. Destruction certification required. d. If the media is damaged and cannot be reused, it is destroyed by methods such as disintegration, incineration, pulverizing, shredding, and/or melting. Destruction certification required. e. If the media is to be reused outside of OSI or an OSI project, Gutmann 35 pass wipe is used prior to reuse.
MP-7	Media Use	<p><u>Control:</u> The organization limits the use of removable media to organization approved devices and prohibits personally owned removable media on all system components. Removable media shall use encryption at the FIPS-2 Level 1.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
MP-7(1)	Media Use	<p><u>MP-7 Control Enhancement:</u></p> <p>(1) MEDIA USE / PROHIBIT USE WITHOUT OWNER</p> <p>The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.</p>
		FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION
PE-1	Physical and Environmental Protection Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all personnel: <ul style="list-style-type: none"> (1) A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Physical and environmental protection policy annually, or upon regulations changes, or from lessons learned from a security event; and 2. Physical and environmental protection procedures annually, or upon policy changes, or from lessons learned from a security event.
PE-2	Physical Access Authorizations	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals monthly or resulting from a security event; and d. Removes individuals from the facility access list when access is no longer required.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
PE-3	Physical Access Control	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Enforces physical access authorizations at facility entry/exit points and additional controls for specified interior areas by; <ul style="list-style-type: none"> 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility and specified interior areas using keys, locks, combinations, card readers, video tapes, alarms, and/or guards; b. Maintains physical access audit logs for all facility entry/exit points and specified interior areas; c. Provides escorted access to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity for meetings and/or maintenance; e. Secures keys, combinations, and other physical access devices; f. Inventories card readers every annually; and g. Changes combinations and keys annually and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.
PE-4	Access Control for Transmission Medium	<p><u>Control:</u> The organization controls physical access to system distribution within organizational facilities using locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.</p>
PE-5	Access Control for Output Devices	<p><u>Control:</u> The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.</p>
PE-6	Monitoring Physical Access	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs monthly and upon occurrence of security violation; and c. Coordinates results of reviews and investigations with the organizational incident response capability.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
PE-6(1)	Monitoring Physical Access	<p><u>PE-6 Control Enhancement:</u></p> <p>(1) <i>MONITORING PHYSICAL ACCESS / INTRUSION ALARMS / SURVEILLANCE EQUIPMENT</i></p> <p>The organization monitors physical intrusion alarms and surveillance equipment.</p>
PE-8	Visitor Access Records	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Maintains visitor access records to the facility where the information system resides for three years; and b. Reviews visitor access records quarterly or when prompted by issue/question.
PE-9	Power Equipment and Cabling	<p><u>Control:</u> The organization protects power equipment and power cabling for the information system from damage and destruction.</p>
PE-10	Emergency Shutoff	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in the computer/server room(s) to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.
PE-11	Emergency Power	<p><u>Control:</u> The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and transition of the information system to long term alternate power or disaster recovery site in the event of a primary power source loss.</p>
PE-12	Emergency Lighting	<p><u>Control:</u> The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.</p>
PE-13	Fire Protection	<p><u>Control:</u> The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.</p>
PE-13(3)	Fire Protection	<p><u>PE-13 Control Enhancement:</u></p> <p>(3) <i>FIRE PROTECTION / AUTOMATIC FIRE SUPPRESSION</i></p> <p>The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
PE-14	Temperature and Humidity Controls	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Maintains temperature and humidity levels within the facility where the information system resides at 70° – 74° F and 40%- 60% relative humidity; and b. Monitors temperature and humidity levels automatically and sends alerts/alarms if there is a variance.
PE-15	Water Damage Protection	<p><u>Control:</u> The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.</p>
PE-16	Delivery and Removal	<p><u>Control:</u> The organization authorizes, monitors, and controls all system components entering and exiting the facility and maintains records of those items.</p>
PE-17	Alternate Work Site	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Employs a minimum level of security standards and procedures for use at alternate work sites such as other government agencies or private residences; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.
		FAMILY: PLANNING
PL-1	Security Planning Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all personnel: <ul style="list-style-type: none"> 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Security planning policy annually; and 2. Security planning procedures quarterly

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
PL-2	System Security Plan	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops a security plan for the information system that: <ul style="list-style-type: none"> 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to all personnel; c. Reviews the security plan for the information system annually or upon lessons learned from security incidents and changes to system security; d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
PL-2(3)	System Security Plan	<p><u>LP-2 Control Enhancement:</u></p> <p>(3) <i>SYSTEM SECURITY PLAN / PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES</i></p> <p>The organization plans and coordinates security-related activities affecting the information system with the data owners, data custodians, system administrators, the Chief Technology Officers, Chief Information Officers, and Information Security Officers before conducting such activities in order to reduce the impact on other organizational entities.</p>
PL-4	Rules of Behavior	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior annually or upon lessons learned from security incident; and d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.
PL-4(1)	Rules of Behavior	<p><u>PL-4 Control Enhancement:</u></p> <p>(1) <i>RULES OF BEHAVIOR / SOCIAL MEDIA AND NETWORKING RESTRICTIONS</i></p> <p>The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
PL-8	Information Security Architecture	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops an information security architecture for the information system that: <ul style="list-style-type: none"> 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture annually or as security architecture changes are made to reflect updates in the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.
		FAMILY: PERSONNEL SECURITY
PS-1	Personnel Security Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all personnel: <ul style="list-style-type: none"> 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Personnel security policy annually or upon regulation change or lessons learned from security incident; and 2. Personnel security procedures annually or upon policy change or lessons learned from security incident.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
PS-2	Position Risk Designation	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations annually or as individuals positions change.
PS-3	Personnel Screening	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to changes in personnel activities, responsibilities, and/or duties.
PS-4	Personnel Termination	<p><u>Control:</u> The organization, upon termination of individual employment:</p> <ul style="list-style-type: none"> a. Disables information system access immediately upon notification (within two hours) and no later than close of termination day; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of nondisclosure agreements and potential limitations on future employment; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies security, receptionists, executives, co-workers, and system administrators within one business day.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
PS-5	Personnel Transfer	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiates (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts by the close of the business of the transition period; c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies security, receptionists, executives, co-workers, and system administrators within one business day.
PS-6	Access Agreements	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements annually; and c. Ensures that individuals requiring access to organizational information and information systems: <ul style="list-style-type: none"> 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or annually.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
PS-7	Third-Party Personnel Security	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify OSI contract manager of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges immediately upon notification (within two hours) or no later than the close of transfer/termination date; and e. Monitors provider compliance.
PS-8	Personnel Sanctions	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies OSI contract manager immediately upon knowledge of the formal employee sanction process (within two hours) or no later than the close of the day the employee's sanction process is initiated when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.
		FAMILY: RISK ASSESSMENT
RA-1	Risk Assessment Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all personnel: <ul style="list-style-type: none"> 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. Risk assessment policy annually or upon regulation changes or lessons learned; and 2. Risk assessment procedures annually or upon policy changes and lessons learned.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
RA-2	Security Categorization	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.
RA-3	Risk Assessment	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in risk assessment report, and issues and risks database; c. Reviews risk assessment results quarterly; d. Disseminates risk assessment results to Project Directors, Information System Administrators, Chief Technology Officers, Chief Information Officers, and Information Security Officers; and e. Updates the risk assessment bi-annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
RA-5	Vulnerability Scanning	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Scans for vulnerabilities in the information system and hosted applications bi-weekly and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: <ol style="list-style-type: none"> 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities; high risk vulnerabilities within 24 to 48 hours, moderate risk vulnerabilities within seven days, and low risk vulnerabilities within 30 days or by the next scheduled change release (whichever is sooner) in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with Chief Technology Officers, Chief Information Officers, and Information Security Officers to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
RA-5(1)	Vulnerability Scanning	<p><u>RA-5 Control Enhancement:</u></p> <p>(1) VULNERABILITY SCANNING / UPDATE TOOL CAPABILITY</p> <p>The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.</p>
RA-5(2)	Vulnerability Scanning	<p><u>RA-5 Control Enhancement:</u></p> <p>(2) VULNERABILITY SCANNING / UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED</p> <p>The organization updates the information system vulnerabilities scanned prior to a new scan and when new vulnerabilities are identified and reported.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
FAMILY: SYSTEMS AND SERVICES ACQUISITION		
SA-1	System and Services Acquisition Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to project management and acquisitions staff: <ul style="list-style-type: none"> 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. System and services acquisition policy annually or upon regulation changes or lessons learned; and 2. System and services acquisition procedures annually or upon policy changes and lessons learned.
SA-2	Allocation of Resources	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Determines information security requirements for the information system or information system service in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
SA-3	System Development Life Cycle	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Manages the information system using system development life cycle best practices, ISO 27004, NIST 800-64, IEEE and PMBOK standards that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities.
SA-4	Acquisition Process	<p><u>Control:</u> The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:</p> <ul style="list-style-type: none"> a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria.
SA-4(1)	Acquisition Process	<p><u>SA-4 Control Enhancement:</u></p> <p>(1) ACQUISITION PROCESS / FUNCTIONAL PROPERTIES OF SECURITY CONTROLS</p> <p>The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
SA-4(2)	Acquisition Process	<p><u>SA-4 Control Enhancement:</u></p> <p class="list-item-l1">(2) ACQUISITION PROCESS / DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS</p> <p>The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality.</p>
SA-4(9)	Acquisition Process	<p><u>SA-4 Control Enhancement:</u></p> <p class="list-item-l1">(9) ACQUISITION PROCESS / FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE</p> <p>The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.</p>
SA-4(10)	Acquisition Process	<p><u>SA-4 Control Enhancement:</u></p> <p class="list-item-l1">(10) ACQUISITION PROCESS / USE OF APPROVED PIV PRODUCTS</p> <p>The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
SA-5	Information System Documentation	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Obtains administrator documentation for the information system, system component, or information system service that describes: <ul style="list-style-type: none"> 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: <ul style="list-style-type: none"> 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and recreate documentation if such documentation is essential to the effective implementation or operation of security controls, and attempt to obtain and determine any remediation/mitigation strategies necessary to otherwise externally protect the system in response; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to system administrators, operational managers, Chief Technology Officers, Chief Information Officers, and Information Security Officers.
SA-8	System Engineering Principles	<p><u>Control:</u> The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
SA-9	External Information System Services	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Requires that providers of external information system services comply with organizational information security requirements and employ the same security standards, procedures, policies, and controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs contracts, audits, and service level agreements to monitor security control compliance by external service providers on an ongoing basis.
SA-9(2)	External Information System Services	<p><u>SA-9 Control Enhancement:</u></p> <p>(2) <i>EXTERNAL INFORMATION SYSTEMS / IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES</i></p> <p>The organization requires providers of all external information systems to identify the functions, ports, protocols, and other services required for the use of such services.</p>
SA-10	Developer Configuration Management	<p><u>Control:</u> The organization requires the developer of the information system, system component, or information system service to:</p> <ul style="list-style-type: none"> a. Perform configuration management during system, component, or service design, development, implementation, and operation; b. Document, manage, and control the integrity of changes to all system components; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to Project Directors or designee, Chief Technology Officers, Chief Information Officers, and Information Security Officers.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
SA-11	Developer Security Testing and Evaluation	<p>Control: The organization requires the developer of the information system, system component, or information system service to:</p> <ul style="list-style-type: none"> a. Create and implement a security assessment plan; b. Perform integration, system, and regression testing/evaluation at full disclosure white box depth; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation.
		FAMILY: SYSTEMS AND COMMUNICATIONS PROTECTION
SC-1	System and Communications Protection Policy and Procedures	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all personnel: <ul style="list-style-type: none"> 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. System and communications protection policy annually or upon regulation changes and lessons learned; and 2. System and communications protection procedures annually or policy changes and lessons learned.
SC-7(3)	Boundary Protection	<p><u>SC-7 Control Enhancement:</u></p> <p>(3) BOUNDARY PROTECTION / ACCESS POINTS</p> <p>The organization limits the number of external network connections to the information system.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
SC-7(4)	Boundary Protection	<p><u>SC-7 Control Enhancement:</u></p> <p>(4) BOUNDARY PROTECTION / EXTERNAL TELECOMMUNICATIONS SERVICES</p> <p>The organization:</p> <ul style="list-style-type: none"> (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy monthly and removes exceptions that are no longer supported by an explicit mission/business need.
SC-12	Cryptographic Key Establishment and Management	<p><u>Control:</u> The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with State Administrative Manual, OSI policy, and NIST 800-152.</p>
SC-17	Public Key Infrastructure Certificates	<p><u>Control:</u> The organization obtains public key certificates from an approved service provider.</p>
SC-18	Mobile Code	<p><u>Control:</u> The organization:</p> <ol style="list-style-type: none"> a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.
SC-19	Voice Over Internet Protocol	<p><u>Control:</u> The organization:</p> <ol style="list-style-type: none"> a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
		FAMILY: SYSTEM AND INFORMATION INTEGRITY POLICY PROCEDURES
SI-1	System and Information Integrity Policy and Procedures	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Develops, documents, and disseminates to all personnel: <ul style="list-style-type: none"> 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: <ul style="list-style-type: none"> 1. System and information integrity policy annually or upon regulation changes or lessons learned; and 2. System and information integrity procedures annually or upon policy changes or lessons learned.
SI-2	Flaw Remediation	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates based on NIST CVSS scores, or CWE of the flaw. Update installation occurs for critical flaws within 24 - 48 hours, priority release within seven days, normal release within 30 days, by the next scheduled change release, or accept risk with an approved risk analysis; and d. Incorporates flaw remediation into the organizational configuration management process.
SI-2(2)	Flaw Remediation	<p><u>SI-2 Control Enhancement:</u></p> <p>(2) <i>FLAW REMEDIATION / AUTOMATED FLAW REMEDIATION STATUS</i></p> <p>The organization employs automated mechanisms weekly to determine the state of information system components with regard to flaw remediation.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
SI-3	Malicious Code Protection	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: <ul style="list-style-type: none"> 1. Perform periodic scans of the information system daily and real-time scans of files from external sources at network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. Blocks malicious code, quarantine malicious code, and send alerts to system administrators, additional to users for workstations in response to malicious code detection; and 3. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
SI-3(1)	Malicious Code Protection	<p><u>SI-3 Control Enhancement:</u></p> <p>(1) <i>MALICIOUS CODE PROTECTION / CENTRAL MANAGEMENT</i></p> <p>The organization centrally manages malicious code protection mechanisms.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls		
Req #	Title	Requirement
SI-4	Information System Monitoring	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Monitors the information system to detect: <ul style="list-style-type: none"> 1. Attacks and indicators of potential attacks in accordance with State Administrative Manual; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides dashboard reports to Chief Technology Officers, Chief Information Officers, and Information Security Officers as needed, but no later than monthly.
SI-4(2)	Information System Monitoring	<p><u>SI-4 Control Enhancement:</u></p> <p>(2) <i>INFORMATION SYSTEM MONITORING / AUTOMATED TOOLS FOR REAL-TIME ANALYSIS</i></p> <p>The organization employs automated tools to support near real-time analysis of events.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
SI-5	Security Alerts, Advisories, and Directives	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Receives information system security alerts, advisories, and directives from US-CERT, Department of Technology Services, the State of California Security Office, MS-ISAC on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: Information System Administrators, Information System Security Officers, Information System Security Managers, Information System Security Engineers, Chief Technology Officers, and Chief Information Officers; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.
SI-7	Software, Firmware, and Information Integrity	<p><u>Control:</u> The organization employs integrity verification tools to detect unauthorized changes to all system components (software, firmware, and information).</p>
SI-7(7)	Software, Firmware, and Information Integrity	<p><u>SI-7 Control Enhancement:</u></p> <p>(7) <i>SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / INTEGRATION OF DETECTION AND RESPONSE</i></p> <p>The organization incorporates the detection of unauthorized changes to established configuration settings and unauthorized elevation of information system privileges into the organizational incident response capability.</p>
SI-8	SPAM Protection	<p><u>Control:</u> The organization:</p> <ul style="list-style-type: none"> a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.
SI-8(1)	SPAM Protection	<p><u>SI-8 Control Enhancement:</u></p> <p>(1) <i>SPAM PROTECTION / CENTRAL MANAGEMENT</i></p> <p>The organization centrally manages spam protection mechanisms.</p>

Baseline Moderate Tailored NIST 800-53 Operational Security Controls

Req #	Title	Requirement
SI-12	Information Handling and Retention	<u>Control:</u> The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

This page intentionally left blank.

Statement of Work Attachment 4

NIST 800-53 Technical Security Controls

Baseline Moderate Tailored NIST 800-53r4 Technical Security Controls
Updated: 16 June 2015

Baseline Moderate Tailored NIST 800-53 Technical Security Controls		
Req #	Title	Requirement
FAMILY: ACCESS CONTROL		
AC-2(2)	Account Management	<u>AC-2 Control Enhancement:</u> (2) ACCOUNT MANAGEMENT / REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS The information system automatically disables temporary and emergency accounts after 48 hours.
AC-2(3)	Account Management	<u>AC-2 Control Enhancement:</u> (3) ACCOUNT MANAGEMENT / DISABLE INACTIVE ACCOUNTS The information system automatically disables inactive accounts after 30 days.
AC-2(4)	Account Management	<u>AC-2 Control Enhancement:</u> (4) ACCOUNT MANAGEMENT / AUTOMATED AUDIT ACTIONS The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies OSI security analyst and contractor security analyst.
AC-3	Access Enforcement	<u>Control:</u> The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
AC-3(7)	Access Enforcement	<u>AC-3 Control Enhancement:</u> (7) ACCESS ENFORCEMENT / ROLE-BASED ACCESS CONTROL The information system enforces a role-based access control policy over defined subjects and objects and controls access based upon project defined roles.

Baseline Moderate Tailored NIST 800-53 Technical Security Controls

Req #	Title	Requirement
AC-4	Information Flow Enforcement	<u>Control:</u> The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on boundary protection policies, e.g. gateways, routers, guards, encrypted tunnels, and firewalls.
AC-6(9)	Least Privilege	<u>AC-6 Control Enhancement:</u> (9) <i>LEAST PRIVILEGE / AUDITING USE OF PRIVILEGED FUNCTIONS</i> The information system audits the execution of privileged functions.
AC-6(10)	Least Privilege	<u>AC-6 Control Enhancement:</u> (10) <i>LEAST PRIVILEGE / PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS</i> The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
AC-7	Unsuccessful Logon Attempts	<u>Control:</u> The information system: a. Enforces a limit of 3 consecutive invalid logon attempts by a user during a 15 minute period; and Automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

Baseline Moderate Tailored NIST 800-53 Technical Security Controls		
Req #	Title	Requirement
AC-8	System Use Notification	<p><u>Control:</u> The information system:</p> <ul style="list-style-type: none"> a. Displays to users a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: <ul style="list-style-type: none"> 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: <ul style="list-style-type: none"> 1. Displays the following system use information: "For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. All activities on this system and related systems are subject to monitoring. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act" for the conditions of use and privacy policy, before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and <p>Includes a description of the authorized uses of the system.</p>
AC-11	Session Lock	<p><u>Control:</u> The information system:</p> <ul style="list-style-type: none"> a. Prevents further access to the system by initiating a session lock after ten minutes of inactivity or upon receiving a request from a user; and <p>Retains the session lock until the user reestablishes access using established identification and authentication procedures.</p>

Baseline Moderate Tailored NIST 800-53 Technical Security Controls		
Req #	Title	Requirement
AC-11(1)	Session Lock	<u>AC-11 Control Enhancement:</u> (1) SESSION LOCK / PATTERN-HIDING DISPLAYS The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.
AC-12	Session Termination	<u>Control:</u> The information system automatically terminates a user session after twenty minutes of inactivity. Note: The application may force a save of the user inputs prior to termination.
AC-17(1)	Remote Access	<u>AC-17 Control Enhancement:</u> (1) REMOTE ACCESS / AUTOMATED MONITORING / CONTROL The information system monitors and controls remote access methods.
AC-17(2)	Remote Access	<u>AC-17 Control Enhancement:</u> (2) REMOTE ACCESS / PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
AC-17(3)	Remote Access	<u>AC-17 Control Enhancement:</u> (3) REMOTE ACCESS / MANAGED ACCESS CONTROL POINTS The information system routes all remote accesses through the minimum number of managed network access control points necessary.
AC-18(1)	Wireless Access	<u>AC-18 Control Enhancement:</u> (1) WIRELESS ACCESS / AUTHENTICATION AND ENCRYPTION The information system protects wireless access to the system using authentication of users, devices, and encryption.
FAMILY: AUDIT AND ACCOUNTABILITY		
AU-3	Content of Audit Records	<u>Control:</u> The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Baseline Moderate Tailored NIST 800-53 Technical Security Controls		
Req #	Title	Requirement
AU-3(1)	Content of Audit Records	<p><u>AU-3 Control Enhancement:</u></p> <p>(1) CONTENT OF AUDIT RECORDS / ADDITIONAL AUDIT INFORMATION</p> <p>The information system generates audit records containing the following additional information: full text recording of privileged commands or the individual identities of group account users.</p>
AU-5	Response to Audit Processing Failures	<p><u>Control:</u> The information system:</p> <ul style="list-style-type: none"> a. Alerts Information System Administrators, Information Security Officers, Information System Security Managers, Information System Security Engineers, and entities that are contractually bound to be notified in the event of an audit processing failure within 2 hours; and b. Takes the following additional actions: overwrite oldest audit records or shut down the information system only upon OSI Project Manager direction.
AU-7	Audit Reduction and Report Generation	<p><u>Control:</u> The information system provides an audit reduction and report generation capability that:</p> <ul style="list-style-type: none"> a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records.
AU-7(1)	Audit Reduction and Report Generation	<p><u>AU-7 Control Enhancement:</u></p> <p>(1) AUDIT REDUCTION AND REPORT GENERATION / AUTOMATIC PROCESSING</p> <p>The information system provides the capability to process audit records for events of interest based on identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed.</p>
AU-8	Time Stamps	<p><u>Control:</u> The information system:</p> <ul style="list-style-type: none"> a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets granularity in hundreds of milliseconds.

Baseline Moderate Tailored NIST 800-53 Technical Security Controls		
Req #	Title	Requirement
AU-8(1)	Time Stamps	<p><u>AU-8 Control Enhancement:</u></p> <p>(1) <i>TIME STAMPS / SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE</i></p> <p>The information system:</p> <ul style="list-style-type: none"> (a) Compares the internal information system clocks Hourly with UTC or GMT; and (b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than one hundredth of a millisecond.
AU-9	Protection of Audit Information	<p><u>Control:</u> The information system protects audit information and audit tools from unauthorized access, modification, and deletion.</p>
AU-12	Audit Generation	<p><u>Control:</u> The information system:</p> <ul style="list-style-type: none"> a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all system components; b. Allows Information Security Officer to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.
FAMILY: CONFIGURATION MANAGEMENT		
CM-7(2)	Least Functionality	<p><u>CM-7 Control Enhancement:</u></p> <p>(1) <i>LEAST FUNCTIONALITY / PREVENT PROGRAM EXECUTION</i></p> <p>The information system prevents program execution in accordance with State Administrative Manual, OSI policies, and rules authorizing the terms and conditions of software program usage.</p>
FAMILY: CONTINGENCY PLANNING		
CP-10(2)	Information System Recovery and Reconstitution	<p><u>CP-10 Control Enhancement:</u></p> <p>(1) <i>INFORMATION SYSTEM RECOVERY AND RECONSTITUTION / TRANSACTION RECOVERY</i></p> <p>The information system implements transaction recovery for systems that are transaction-based.</p>
FAMILY: IDENTIFICATION AND AUTHENTICATION		

Baseline Moderate Tailored NIST 800-53 Technical Security Controls		
Req #	Title	Requirement
IA-2	Identification and Authentication (Organization Users)	<p><u>Control:</u> The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).</p>
IA-2(1)	Identification and Authentication (Organization Users)	<p><u>IA-2 Control Enhancement:</u></p> <p>(1) <i>IDENTIFICATION AND AUTHENTICATION / NETWORK ACCESS TO PRIVILEGED ACCOUNTS</i> The information system implements multifactor authentication for network access to privileged accounts.</p>
IA-2(2)	Identification and Authentication (Organization Users)	<p><u>IA-2 Control Enhancement:</u></p> <p>(2) <i>IDENTIFICATION AND AUTHENTICATION / NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS</i> The information system implements multifactor authentication for network access to non-privileged accounts.</p>
IA-2(3)	Identification and Authentication (Organization Users)	<p><u>IA-2 Control Enhancement:</u></p> <p>(3) <i>IDENTIFICATION AND AUTHENTICATION / LOCAL ACCESS TO PRIVILEGED ACCOUNTS</i> The information system implements multifactor authentication for local access to privileged accounts.</p>
IA-2(8)	Identification and Authentication (Organization Users)	<p><u>IA-2 Control Enhancement:</u></p> <p>(8) <i>IDENTIFICATION AND AUTHENTICATION / NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT</i> The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.</p>
IA-2(11)	Identification and Authentication (Organization Users)	<p><u>IA-2 Control Enhancement:</u></p> <p>(11) <i>IDENTIFICATION AND AUTHENTICATION / REMOTE ACCESS - SEPARATE DEVICE</i> The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets cryptographic identification device.</p>

Baseline Moderate Tailored NIST 800-53 Technical Security Controls

Req #	Title	Requirement
IA-2(12)	Identification and Authentication (Organization Users)	<p><u>IA-2 Control Enhancement:</u></p> <p>(12) <i>IDENTIFICATION AND AUTHENTICATION / ACCEPTANCE OF PIV CREDENTIALS</i></p> <p>The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.</p>
IA-3	Device Identification and Authentication	<p><u>Control:</u> The information system uniquely identifies and authenticates laptops, tablets, and smart phones before establishing a local, remote, and/or network connection.</p>
IA-5(1)	Authenticator Management	<p><u>IA-5 Control Enhancement:</u></p> <p>(1) <i>AUTHENTICATOR MANAGEMENT / PASSWORD-BASED AUTHENTICATION</i></p> <p>The information system, for password-based authentication:</p> <ul style="list-style-type: none"> (a) Enforces minimum password complexity of at least eight characters, and at least one character from three of these four categories: uppercase letters, lower case letters, numbers, and special characters; (b) Enforces at least the following number of changed characters when new passwords are created: At least half of the characters are different from previous password; (c) Stores and transmits only cryptographically-protected passwords; (d) Enforces password minimum and maximum lifetime restrictions of minimum of one day and a maximum of sixty days; (e) Prohibits password reuse for 12 generations; and (f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Baseline Moderate Tailored NIST 800-53 Technical Security Controls		
Req #	Title	Requirement
IA-5(2)	Authenticator Management	<p><u>IA-5 Control Enhancement:</u></p> <p>(2) AUTHENTICATOR MANAGEMENT / PKI-BASED AUTHENTICATION</p> <p>The information system, for PKI-based authentication:</p> <ul style="list-style-type: none"> (a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; (b) Enforces authorized access to the corresponding private key; (c) Maps the authenticated identity to the account of the individual or group; and (d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.
IA-5(11)	Authenticator Management	<p><u>IA-5 Control Enhancement:</u></p> <p>(11) AUTHENTICATOR MANAGEMENT HARDWARE TOKEN-BASED AUTHENTICATION</p> <p>The information system, for hardware token-based authentication, employs mechanisms that are Radius compatible. Soft tokens can also be accepted.</p>
IA-6	Authenticator Feedback	<p><u>Control:</u> The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.</p>
IA-7	Cryptographic Module Authentication	<p><u>Control:</u> The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.</p>
IA-8	Identification and Authentication (Non-Organizational Users)	<p><u>Control:</u> The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).</p>
IA-8(1)	Identification and Authentication (Non-Organizational Users)	<p><u>IA-8 Control Enhancement:</u></p> <p>(1) IDENTIFICATION AND AUTHENTICATION / ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES</p> <p>The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.</p>

Baseline Moderate Tailored NIST 800-53 Technical Security Controls		
Req #	Title	Requirement
IA-8(2)	Identification and Authentication (Non-Organizational Users)	<u>IA-8 Control Enhancement:</u> (2) <i>IDENTIFICATION AND AUTHENTICATION / ACCEPTANCE OF THIRD-PARTY CREDENTIALS</i> The information system accepts only FICAM-approved third-party credentials.
IA-8(4)	Identification and Authentication (Non-Organizational Users)	<u>IA-8 Control Enhancement:</u> (3) <i>IDENTIFICATION AND AUTHENTICATION / USE OF FICAM-ISSUED PROFILES</i> The information system conforms to FICAM-issued profiles.
		FAMILY: MEDIA PROTECTION
MP-5(4)	Media Transport	<u>MP-5 Control Enhancement:</u> (4) <i>MEDIA TRANSPORT / CRYPTOGRAPHIC PROTECTION</i> The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.
		FAMILY: RISK ASSESSMENT
RA-5(5)	Vulnerability Scanning	<u>RA-5 Control Enhancement:</u> (5) <i>VULNERABILITY SCANNING / PRIVILEGED ACCESS</i> The information system implements privileged access authorization to all system components for all scanning activities.
		FAMILY: SYSTEMS AND COMMUNICATIONS PROTECTION
SC-2	Application Partitioning	<u>Control:</u> The information system separates user functionality (including user interface services) from information system management functionality.
SC-4	Information in Shared Resources	<u>Control:</u> The information system prevents unauthorized and unintended information transfer via shared system resources.
SC-5	Denial of Service Protection	<u>Control:</u> The information system protects against or limits the effects of the denial of service attacks: by employing firewalls, IDS/IPS, etc..

Baseline Moderate Tailored NIST 800-53 Technical Security Controls		
Req #	Title	Requirement
SC-7	Boundary Protection	<u>Control:</u> The information system: <ol style="list-style-type: none"> Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; Implements subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
SC-7(5)	Boundary Protection	<u>SC-7 Control Enhancement:</u> <p>(3) BOUNDARY PROTECTION / DENY BY DEFAULT / ALLOW BY EXCEPTION</p> <p>The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).</p>
SC-7(7)	Boundary Protection	<u>SC-7 Control Enhancement:</u> <p>(7) BOUNDARY PROTECTION / PREVENT SPLIT TUNNELING FOR REMOTE DEVICES</p> <p>The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.</p>
SC-8	Transmission Confidentiality and Integrity	<u>Control:</u> The information system protects the confidentiality, integrity, and availability of transmitted information.
SC-8(1)	Transmission Confidentiality and Integrity	<u>SC-8 Control Enhancement:</u> <p>(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY / CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION</p> <p>The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information during transmission.</p>
SC-10	Network Disconnect	<u>Control:</u> The information system terminates the network connection associated with a communications session at the end of the session or after fifteen minutes of inactivity.

Baseline Moderate Tailored NIST 800-53 Technical Security Controls		
Req #	Title	Requirement
SC-13	Cryptographic Protection	<u>Control:</u> The information system implements FIPS 199 validated cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
SC-15	Collaborative Computing Devices	<u>Control:</u> The information system: <ol style="list-style-type: none"> Prohibits remote activation of collaborative computing devices with the following exceptions: devices requested via a non-standards exemption request; and Provides an explicit indication of use to users physically present at the devices.
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	<u>Control:</u> The information system: <ol style="list-style-type: none"> Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	<u>Control:</u> The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.
SC-22	Architecture and Provisioning for Name/Address Resolution Service	<u>Control:</u> The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.
SC-23	Session Authenticity	<u>Control:</u> The information system protects the authenticity of communications sessions.
SC-28	Protection of Information at Rest	<u>Control:</u> The information system protects the confidentiality, integrity, and availability of all project data (PHI, PII).
SC-39	Process Isolation	<u>Control:</u> The information system maintains a separate execution domain for each executing process.

Baseline Moderate Tailored NIST 800-53 Technical Security Controls		
Req #	Title	Requirement
		FAMILY: SYSTEM AND INFORMATION INTEGRITY POLICY PROCEDURES
SI-3(2)	Malicious Code Protection	<u>SI-3 Control Enhancement:</u> <p>(1) MALICIOUS CODE PROTECTION / AUTOMATIC UPDATES The information system automatically updates malicious code protection mechanisms.</p>
SI-4(4)	Information System Monitoring	<u>SI-4 Control Enhancement:</u> <p>(4) INFORMATION SYSTEM MONITORING / INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC The information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions.</p>
SI-4(5)	Information System Monitoring	<u>SI-4 Control Enhancement:</u> <p>(5) INFORMATION SYSTEM MONITORING / SYSTEM-GENERATED ALERTS The information system alerts Chief Technology Officers and system administrators when the following indications of compromise or potential compromise occur: from IDS and IPS alerts, and system outage alerts.</p>
SI-7(1)	Software, Firmware, and Information Integrity	<u>SI-7 Control Enhancement:</u> <p>(1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / INTEGRITY CHECKS The information system performs an integrity check of software and operating systems at startup, restart, shutdown, and abort.</p>
SI-8(2)	SPAM Protection	<u>SI-8 Control Enhancement:</u> <p>(1) SPAM PROTECTION / AUTOMATIC UPDATES The information system automatically updates spam protection mechanisms.</p>
SI-10	Information Input Validation	<u>Control:</u> The information system checks the validity of all system inputs.
SI-11	Error Handling	<u>Control:</u> The information system: <ul style="list-style-type: none"> a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to the system administrators and the Information System Security Engineer.

Baseline Moderate Tailored NIST 800-53 Technical Security Controls

Req #	Title	Requirement
SI-16	Memory Protection	<u>Control:</u> The information system implements hardware enforced data execution prevention safeguards to protect its memory from unauthorized code execution.

Statement of Work Attachment I Special Provisions

Supplemental Contracts:

The State may undertake or award supplemental contracts for work related to this Contract or any portion thereof. Contractor shall fully cooperate with such other contractors and the State in all such cases. To the extent that such cooperation requires additional work on Contractor's part which is unanticipated, the Parties will follow the Work Authorization process.

Limitation of Authority:

Waivers - Only the State Project Director or designee (with the delegation to be made in writing prior to action) shall have the express, implied, or apparent authority to waive any clause or condition of this Contract on behalf of the State. Any waiver of any clause or condition of this Contract is not effective or binding until made in writing and signed by the State Project Director or designee thereof and approved by the California Department of Technology.

Changes - The State Project Director or designee is the only individual that may authorize changes to this Contract in accordance with Paragraph 84 or a Contract amendment. The State Project Director or designee shall delegate in writing authority to authorize changes prior to any changes. All such changes shall be made in writing and approved by the California Department of Technology. Any change proposed by any other State employee or an employee of any County shall be of no effect.

Contractor Staff: During the Contract term, the State reserves the right to approve or disapprove Contractor's staff, including, but not limited to, any subcontractor staff assigned to this Contract, or to approve or disapprove any proposed changes in staff or staffing levels. The State may request, and the Contractor will remove from work on the Project, Contractor employees or subcontractors who the State identifies as being incompetent, careless, insubordinate, unsuitable, or otherwise unacceptable, or whose continued employment on the Project is deemed to be contrary to the public interest or not in the best interest of the State, provided that such request will be based solely on nondiscriminatory reasons and Contractor shall have the right to request the withdrawal of any such request upon a showing to the State that the concern is unfounded. Upon request of the State Project Director or designee, Contractor shall provide the State with a resume of any member of its staff or a Subcontractor's staff assigned to or proposed to be assigned to any aspect of the performance of this Contract prior to commencing any services.

Key Staff:

Initial Key Staff - Except as provided below, the Key Staff identified in the Contractor's Proposal shall be the Key Staff assigned to this Project as of the effective date of this Contract. The key personnel specified in this contract are considered to be essential to work performance. Except as provided below, no substitution or replacement of the key personnel shall be approved within the first ninety (90) days after contract award.

Contractor Reassignment of Key Staff - During the term of this Contract, including any period of time for which a Stop Work Order is issued, Contractor shall not make changes in the

assignment of its Key Staff except in the event of death, illness, retirement, disability, termination, or leaving Contractor's employment and not serving as a consultant or contractor to Contractor, or subject to mutual agreement by the Parties to allow for removal. If a member of Contractor's Key Staff is unable to perform due to factors beyond Contractor's reasonable control (e.g., illness, resignation), Contractor will use its best efforts in promptly providing suitable substitute personnel.

Replacement of Key Staff - In the event replacement of Key Staff is required in accordance with Contractor's Reassignment of Key Staff above, the Contractor shall provide the Project Director with the proposed replacement candidate's resume within 7 Calendar Days of the date the Key Staff member becomes unavailable and allow the Project Director the opportunity to interview and approve the candidate.

The Project Director or designee may request that Contractor replace a Key Staff member and shall advise Contractor in writing of the basis for the request. In such event, Contractor shall provide a proposed replacement candidate's resume within 7 Calendar Days of the date the requested replacement is made by the State.

When Key Staff is replaced by Contractor or by the State, the State shall have the right to contact references and evaluate information provided and determine if the Key Staff substitution or replacement is acceptable. Any substitution or replacement Key Staff shall have equal or better qualifications when compared to the Key Staff that is being replaced.

Deliverables:

Contractor shall use the Contractor's expert knowledge and this Contract as the basis for the development of the Deliverables. The Parties acknowledge that Deliverables and services may be added in the future and agree to work together to identify the contents of and Acceptance Criteria for any additional Deliverables as a Work Authorization.

Notwithstanding CWS-NS General Provisions Paragraph 16 - Inspection, Acceptance and Rejection, the following process will be used for inspection, Acceptance, and rejection of Deliverables in this Contract.

Right to Inspect - The Deliverables and services being provided by the Contractor and its subcontractors, if any, pursuant to this Contract shall be available for inspection and review at any reasonable time by representatives of the State. Such Deliverables, including but not limited to source code, shall be maintained in a reasonably current state and made available to the State on a continuous basis in an electronic repository. Contractor shall retain backup copies in writing and on electronic media of all Products and shall provide the State on its request with a copy thereof until that time.

Contractor shall deliver all Deliverables pursuant to this Contract to the State Project Director or designee at the State Project Office for purposes of determining whether the State will give its Acceptance for such Deliverables. The State's review of Deliverables will be in accordance with the timeframes set forth in the Product Roadmap. The State's review period will vary with the complexity and volume of the Deliverable. The State will have at least 10 Business Days for such review, with the first day starting on the next Business Day after delivery. If the State does not provide such notice of rejection within 10 Business Days of delivery, such Deliverables and services will be deemed accepted by the State. Acceptance by the State will be final and irreversible, except as it relates to latent defects, fraud, and gross mistakes amounting to fraud.

Acceptance shall not be construed to waive any warranty rights that the State might have at law or by express reservation in this Contract with respect to any nonconformity.

Effect of Acceptance - By submitting a Deliverable or performing a service, the Contractor represents that the Deliverable or service meets the requirements of this Contract. The Parties acknowledge and agree that the State's Acceptance of a Deliverable or service indicates only that it has reviewed the Deliverable or service and detected no Deficiencies at that time and that the State's Acceptance of a Deliverable or service does not discharge the Contractor's obligations to ensure comprehensiveness, functionality, or effectiveness of the Module as a whole or in any way lessen the Contract requirements. The Parties agree that the Contract requirements shall be modified only through an Agile Sprint Planning and User Story Acceptance Process, a Work Authorization, or an amendment to this Contract.

Acceptance - The State will provide Acceptance for the Deliverable or service if it meets the Acceptance Criteria for each Deliverable or service.

Work Authorization

The State Project Director may, at any time, by written Work Authorization make changes within the general scope of this Contract if the State Project Director determines that such changes are necessary to the successful accomplishment of the Project and is within the Statement of Work, the procedures outlined in this paragraph will be employed. For each item, a Work Authorization will be prepared in accordance with the sample Work Authorization attached as Attachment XX to this Contract. For purposes of Paragraph 11 of the CWS-NS General Provisions, a Work Authorization shall be considered to be a Contract form.

Work Authorization Approval Process -

For each change in work requirements, a Work Authorization shall be prepared. Either party may initiate a proposal for a Work Authorization.

Contractor shall respond in writing to a Work Authorization issued by the State Project Director within the time mutually agreed to by the Parties or such longer time allowed by the State Project Director in writing. Each Work Authorization response shall contain:

- A. A statement of the purpose, objective, or goals to be performed by the Contractor;
- B. A full work description;
- C. The job classification or approximate skill level of the staff to be made available by Contractor;
- D. An identification of all Deliverables to be developed by Contractor and delivered to the State;
- E. An identification of all significant materials to be delivered by the State to Contractor;
- F. A time schedule for the provisions of identified Deliverables or services by Contractor;
- G. Acceptance Criteria for the work to be performed;
- H. The name or identification of Contractor staff to be assigned;
- I. Contractor's work hours required to accomplish the purpose, objective, or goals; and
- J. Contractor's estimated total cost of the Work Authorization.

Inclusion in Contract –

All Work Authorizations must be in writing, signed by the State Project Director prior to beginning work. Upon Acceptance by the State Project Director, each such Work Authorization

shall be incorporated into and become a part of the Contract and the terms of this Contract shall apply to all such Work Authorizations. In no event shall a Work Authorization be deemed a separate contract.

Prior Approval - In the event any single Work Authorization or the total costs of all Work Authorizations equals or exceeds ten (10) percent of the total Contract value, prior approval of the State's control agencies is required through an approved Contract amendment prior to the Work Authorization becoming effective.

Disagreement - If the Parties are unable to reach an agreement in writing within 10 Business Days of Contractor's response to a Work Authorization, the State Project Director may make a determination of the price and schedule for the Work Authorization, and Contractor shall proceed with the work according to that price and schedule, which shall be included in the resulting Work Authorization, subject to Contractor's right to dispute the State Project Director's determination of the price or schedule using the dispute resolution process under Paragraph 44 of the CWS-NS General Provisions.

Services - Contractor shall perform all services required pursuant to this Contract in a professional manner, with high quality, using best industry practices, such as the Institute of Electrical and Electronics Engineers (IEEE), American National Standards Institute (ANSI), International Standards Organization/International Electrotechnical Commission (ISO/IEC), and Project Management Institute (PMI) standards, and in accordance with the standards of the manufacturers of applicable systems' components.

Assistance During Termination: Prior to termination or expiration of this Contract, each party will assist the other party in the orderly termination of this Contract and the transfer of all assets, tangible and intangible, and of all services, as may facilitate the orderly, nondisrupted continuation of the Project. Towards this end, Contractor shall assist the State at the State's request in transitioning the Services to another contractor.

Ownership and Rights: The following items are property of the State: all data, documents, graphics and code created pursuant to this Contract, including but not limited to, plans, reports, schedules, schemas, metadata, architecture designs, and the like; new Open Source Software created by the contractor and forks or branches, where permitted, of current Open Source Software where the contractor has made a modification; new tooling, scripting configuration management, infrastructure as code, or any other final changes or edits to successfully deploy or operate the software. For the property listed above, the State shall provide an open-source license of its choosing.

Contractor Use of Technology:

Except with written approval of the State Project Director, the Contractor shall use Open Source Software wherever possible. The Open Source Software chosen by Contractor must receive Acceptance by the State Project Director or designee prior to use. All licenses shall be expressly listed in the Deliverable. Regardless of license(s) used (e.g., MIT, GPL, Creative Commons 0), the license(s) shall be clearly listed in the Deliverable. If the contractor must use Software that does not have an Open Source Software license, the contractor shall request and must receive Approval from the State Project Director before using that Software for performance under this Contract. If approved, all licenses shall be clearly set forth in a conspicuous place, as determined by the State, when work is delivered to the State.

If a technical specification or documentation of the Open Source Software provides implementation guidance, the Contractor shall comply with that guidance. If implementation guidance is not provided, the Contractor shall attach or include the license within the work itself (e.g., code comments at the beginning of a file or contained in a license file within a software repository).

The Contractor shall develop all custom software written pursuant to this Contract in the open from the first Calendar Day of Development.

Confidential Information:

State Test Data and Personal Identifying Information - The State shall provide test data for use by Contractor to develop the module. Contractor shall not have access to Confidential Information or production data unless the State Project Director or designee specifically authorizes, in writing access, to the Confidential Information or production data.

Access and Nondisclosure Obligation - During the term of this Contract, Contractor and the State will have access to and become acquainted with Confidential Information of the other Party. In addition to the requirements imposed on Contractor by CWS-NS General Provision - Information Technology paragraph 34, the State and Contractor, and each of their officers, employees and agents, shall maintain all Confidential Information of the other party in strict confidence and shall not at any time use, publish, reproduce or disclose any Confidential Information, except to authorized employees, contractors, or agents requiring such information, as authorized in writing by the other party, to perform its obligations as authorized hereunder, or unless otherwise required by law.

Protective Measures - Both Parties shall take steps to safeguard the other party's Confidential Information against unauthorized disclosure, reproduction, publication, or use. Contractor shall have written policies governing access to, duplication, and dissemination of all such Confidential Information. Contractor shall take appropriate action, as reasonably determined by the State, with any persons permitted access to the State's Confidential Information so as to enable Contractor to hold the Confidential Information in strict confidence and otherwise to satisfy Contractor's obligations under this Contract. The use or disclosure by either party of any Confidential Information concerning the other party for any purpose not directly connected with the administration of the disclosing Parties responsibilities with respect to service(s) provided under this Contract is prohibited except by prior written consent of the other Party, unless otherwise required by law.

Security Requirements - Contractor, its officers, employees, and Subcontractors shall at all times comply with all security standards, practices, and procedures that are equal to or exceed those of the State, including without limitation the California Department of Social Services' Confidentiality and Security Requirements, and which the State may establish from time to time, with respect to information and materials that come into Contractor's possession and to which Contractor gains access under this Contract. Such information and materials include, without limitation, all Confidential Information.

Unauthorized Disclosure of Confidential Information - Each Party will immediately report to the other Party any and all unauthorized disclosures or uses of the other Party's Confidential Information of which it or its staff is aware or has knowledge. Each Party acknowledges that any publication or disclosure of the other Party's Confidential Information to others may cause

immediate and irreparable harm to the other Party, and if either Party should publish or disclose such Confidential Information to others without authorization, the other Party shall immediately be entitled to injunctive relief to prevent further harm.

Public Records Act - Notwithstanding anything to the contrary herein, the Contractor acknowledges that this Contract shall be a public record under State law. Any specific information that is claimed by the Contractor to be Confidential Information shall be clearly identified as such by the Contractor. To the extent consistent with State law, the State will maintain the confidentiality of all such information marked as Confidential Information.

Request for Disclosure - The State will notify the Contractor as soon as reasonably practicable of any and all public records requests for the Contractor's Confidential Information in accordance with and subject to applicable State laws regarding disclosure of the Contractor's Confidential Information. If the Contractor disagrees with the State's disclosure of the Contractor's Confidential Information, the Contractor shall have the right to contest its disclosure in accordance with State law. If the Contractor fails to obtain a court order enjoining disclosure, the State will release the identified requested information on the date specified in the order.

Exceptions - The following information shall not be considered Confidential Information for the purposes of this Contract:

- i) Information which was already known to the receiving party, other than under an obligation of confidentiality, at the time of disclosure by the disclosing party; information which was generally available to the public or otherwise part of the public domain at the time of its disclosure to the receiving party;
 - ii) Information which now is or hereafter becomes publicly known by other than a breach hereof;
 - iii) information which is developed by one party independently of any disclosures made by the other party of such information;
- Information
- iv) Information which was received by the receiving party after disclosure to it from a third party who had a lawful right to disclose such information to it; or
 - v) Information which is disclosed by a party pursuant to subpoena or other legal process and which as a result becomes lawfully obtainable by the public. The party who receives such a subpoena shall promptly notify the other party.

Written Staff Contracts - Contractor agrees to require staff to which Contractor makes available the State's Confidential Information to agree in writing to observe and perform all provisions of this Confidential Information paragraph. Submission by the Contractor to the State Project Director of Contractor's current internal process for ensuring the protection of Confidential Information substantially meets the requirements of this paragraph.

Survival - The provisions of this entire Paragraph, Confidential Information, shall remain in effect following the termination or expiration of this Contract.

Counties Are Independent Entities:

California Counties and Tribes are independent and separate legal entities from the State. As a result, any particular County or Tribe's preparedness, cooperation, and success in becoming operational with the Module or CWS-NS solution is beyond the control of Contractor or the State. The State shall not be liable to Contractor or in default under this Contract if a County is not prepared or is late in becoming operational with the Module or CWS-NS as scheduled and Contractor shall not be liable for delays caused by a County.

Engagement of Personnel with Criminal Records:

The Contractor agrees not to engage or continue to engage any persons for the purpose of fulfilling the requirements of this Contract if (1) they have a conviction or have pleaded nolo contendere to a crime, or have committed an act involving dishonesty, fraud, or deceit, if the crime or act is substantially related to the qualifications, functions, or duties of the position, or (2) they have been convicted or arrested for a crime, and are free on bail or on their own recognizance pending trial or appeal, where the alleged or actual crime has a reasonable nexus to the information or data to which the contractor shall have access. For the purposes of this paragraph, data includes the State's records, client information, files, forms, and financial, statistical, personal, personnel, technical and other sensitive information that will be processed by the Software or that originates from or is provided by the State in connection with this Contract. In addition, Contractor shall conduct a criminal background or Live Scan on all Contractor and Subcontractor staff that will have access to any criminal history background information in the course and scope of their responsibilities related to this Contract. Within 15 business days of contract award, or immediately following the addition of new staff, the Contractor shall provide a written statement to the State Project Director certifying that such staff have not committed or been arrested for any of the acts or crimes as outlined above. Additionally, during the term of the contract, the Contractor must notify the State Project Director immediately upon becoming aware of a staff's arrest or conviction that was not previously documented. The Contractor shall maintain the confidentiality of information gathered under this provision and use it solely to promote the security of the CWS-NS System.

Remedies:

Except for remedies specifically designated as exclusive, no remedy conferred by any of the specific provisions of this Contract is intended to be exclusive of any other remedy, and each and every remedy shall be cumulative and shall be in addition to every other remedy given hereunder, now or hereafter existing at law or in equity or by statute or otherwise. The election of any one or more remedies by either Party shall not constitute a waiver of the right to pursue other available remedies.

Subcontractors:

Contractor may enter into subcontracts with third parties for the performance of any part of Contractor's duties and obligations. Contractor is responsible and liable for the proper performance of and the quality of any work performed by any and all subcontractors. In addition, the Contractor's use of any subcontractor shall not cause the loss of any warranty from the Contractor or any software manufacturer or provider. The State reserves the right to reject or refuse admission to any Contractor or subcontractor staff whose workmanship, in the reasonable judgment of the State, is deemed to be substandard. In no event shall the existence of a subcontract operate to release or reduce the liability of Contractor to the State for any breach in the performance of Contractor's duties. .

Direct Agreements - Upon expiration or termination of this Contract for any reason, the State shall have the right to enter into direct agreements with any of the subcontractors as permitted by law. Contractor agrees that its arrangements with subcontractors will not prohibit or restrict such subcontractors from entering into direct agreements with the State.

Survival:

The terms, conditions and warranties contained in this Contract that by their sense and content are intended to survive the performance hereof by the Parties shall so survive the completion of the performance, cancellation or termination of this Contract. In addition, the terms of the following paragraphs shall survive termination of this Contract: CWS-NS General Provisions Paragraph 26 (Limitation of Liability), Paragraph 28 (Indemnification), Paragraph 34 (Confidentiality of Data), and Paragraphs 21, 22, 23 (termination).

Third Party Beneficiaries: It is expressly understood and agreed that the enforcement of the terms and conditions of this Contract and all rights of action relating to such enforcement, shall be strictly reserved to the State and Contractor. Nothing contained in this Contract shall give to or allow any claim or right of action whatsoever by any third person. It is the express intention of the State and Contractor that any person or entity, other than the State or Contractor, receiving services or benefits shall be deemed an incidental beneficiary only, except as otherwise provided in the Paragraphs entitled Rights in Work Product and Software License of the CWS-NS General Provisions.

Question and Answers for Solicitation #RFP OSI 31326-- Child Welfare Services New System API Module

Overall Solicitation Questions

There are no questions associated with this Solicitation.

Question Deadline: Jan 8, 2016 5:00:00 PM PST