

Agenda



County of Inyo Board of Supervisors

Board of Supervisors Room
County Administrative Center
224 North Edwards
Independence, California

All members of the public are encouraged to participate in the discussion of any items on the Agenda. Anyone wishing to speak, please obtain a card from the Board Clerk and indicate each item you would like to discuss. Return the completed card to the Board Clerk before the Board considers the item (s) upon which you wish to speak. You will be allowed to speak about each item before the Board takes action on it.

Any member of the public may also make comments during the scheduled "Public Comment" period on this agenda concerning any subject related to the Board of Supervisors or County Government. No card needs to be submitted in order to speak during the "Public Comment" period.

Public Notices: (1) In Compliance with the Americans with Disabilities Act, if you need special assistance to participate in this meeting please contact the Clerk of the Board at (760) 878-0373. (28 CFR 35.102-35.104 ADA Title II). Notification 48 hours prior to the meeting will enable the County to make reasonable arrangements to ensure accessibility to this meeting. Should you because of a disability require appropriate alternative formatting of this agenda, please notify the Clerk of the Board 72 hours prior to the meeting to enable the County to make the agenda available in a reasonable alternative format. (Government Code Section 54954.2). (2) If a writing, that is a public record relating to an agenda item for an open session of a regular meeting of the Board of Supervisors, is distributed less than 72 hours prior to the meeting, the writing shall be available for public inspection at the Office of the Clerk of the Board of Supervisors, 224 N. Edwards, Independence, California and is available per Government Code § 54957.5(b)(1).

Note: Historically the Board does break for lunch; the timing of a lunch break is made at the discretion of the Chairperson and at the Board's convenience.

December 19, 2017

8:30 a.m. 1. PUBLIC COMMENT

CLOSED SESSION

- 2. CONFERENCE WITH LEGAL COUNSEL – ANTICIPATED LITIGATION** – Initiation of litigation pursuant to paragraph (4) of subdivision (d) of Government Code §54956.9 (two cases).
- 3. CONFERENCE WITH REAL PROPERTY NEGOTIATORS [Pursuant to Government Code §54956.8]** – Property: APN 010-490-12, Bishop, California. Agency Negotiators: Kevin Carunchio, County Administrator; and Marshall Rudolph, County Counsel. Negotiating Parties: Inyo County and Inyo County Development LLC. Under Negotiations: price and terms of payment.

OPEN SESSION (With the exception of timed items, all open-session items may be considered at any time and in any order during the meeting in the Board's discretion.)

10:00 a.m. PLEDGE OF ALLEGIANCE

- 4. REPORT ON CLOSED SESSION**
- 5. PUBLIC COMMENT**
- 6. COUNTY DEPARTMENT REPORTS** (Reports limited to two minutes)
- 7. PRESENTATION** – The County Administrator will announce the winners of the Fifth Annual Inyo County Offices Holiday Door Decoration Contest.
- 8. INTRODUCTIONS** – The following new employees will be introduced to the Board: Jean Bigham, Integrated Caseworker III, Marissa D. Hobbs, Registered Nurse, and Timothy Whitney, In-Home Supportive Services Nurse, HHS.

CONSENT AGENDA (Approval recommended by the County Administrator)

COUNTY ADMINISTRATOR

9. Request Board approve a purchase order to OKU Solutions in an amount not to exceed \$20,000 for costs associated with cell tower site mapping and related services.
10. **Information Services** – Request Board approve Inyo County's participation in the Local Update Census Addresses (LUCA) Operation in support of the U.S. Census Bureau's decennial census of 2020.

PUBLIC WORKS

11. Request Board approve a resolution titled, "A Resolution of the Board of Supervisors of the County of Inyo, State of California Authorizing the Recording of a Notice of Completion for the Water Department Roof Sealing Project."
12. Request Board approve Amendment 2 to current Standard Contract No. 116 with Wilder Barton for the operation and maintenance of the Independence, Laws and Lone Pine town water systems, extending the term through December 31, 2018, unless terminated earlier, and increasing the total contract amount not to exceed \$924,300, contingent upon the Board's adoption of future budgets; and authorize the Chairperson to sign, contingent upon all appropriate signatures being obtained.

DEPARTMENTAL (To be considered at the Board's convenience)

13. **AUDITOR-CONTROLLER** – Request Board approve the Second Review of the Social Security Number Truncation Program report prepared by the Auditor's Office.
14. **CLERK-RECORDER** – Request Board: A) authorize the Clerk-Recorder to enter into a contract with Dominion Voting Systems, Inc. of Denver, CO for the provision of New Voting System in an amount not to exceed \$201,796 plus shipping for the period of the Agreement-effective date through December 31, 2025; B) declare Dominion Voting Systems, Inc. the sole-source provider for a New Voting System and Managed Services related to the New Voting System; and C) amend the Fiscal Year 2017-2018 Election Innovations Budget (Budget 500202) as follows: increase appropriation in Equipment (Object Code 5650) by \$211,796 (*4/5ths vote required*).
15. **HEALTH & HUMAN SERVICES – Behavioral Health** – Request Board ratify and approve the performance contract between Inyo County Mental Health and the State of California, Department of Health Care Services for the provision of county mental health services for the one-year period of July 1, 2017 through June 30, 2018 and authorize the HHS Deputy Director of Behavioral Health, in her role as the County Mental Health Director, to sign both copies of each contract as well as complete the Certification Clause.
16. **HEALTH & HUMAN SERVICES – First 5** – Request Board: A) approve amended bylaws for the First 5 Children and Families Commission adding an alternate member of the Board of Supervisors to its composition; and either B) appoint from your membership an alternate member to the First 5 Children and Families Commission to fill the 2017 calendar year alternate position for the remainder of 2017; or C) choose to delay the alternate appointment until the Board makes its 2018 committee appointments in January.
17. **HEALTH & HUMAN SERVICES – First 5** – Request Board appoint and/or reappoint the following individuals to the First 5 Children and Families Commission:
 - Eileen Dougherty to an unexpired three-year term ending December 5, 2018 to be filled by a parent;
 - Amanda Miloradich to an unexpired term ending December 5, 2018 to be filled by someone with experience in the early health field;
 - Robyn Wisdom to a three-year term ending December 5, 2020 to be filled by a specialist in early childhood development;
 - Melissa Best-Baker to an unexpired three-year term ending April 20, 2020 to be filled by the designee of the Health and Human Services Director, as defined in Health and Safety Code Section 130140; and
 - Anna Scott to an unexpired three-year term ending April 20, 2020 to be filled by the Health and Human Services Director or his/her designee.

(Notices of Vacancy resulted in responses from the above-named individuals.)
18. **PUBLIC WORKS** – Request Board receive report from staff on the status of the Independence Town Water System Transmission Main and authorize staff to proceed with emergency repairs.
19. **PUBLIC WORKS** – Request Board amend the Fiscal Year 2017-2018 Bishop Airport Apron Budget (Budget 630304) as follows: increase estimated revenue in Federal Grants (Object Code 4555) by \$154,375 and increase appropriations in Professional Services (Object Code 5265) by \$154,375 (*4/5ths vote required*).

20. **PUBLIC WORKS** – Request Board ratify and approve the Lease Agreement between the County of Inyo and Eastern Sierra Transit Authority, JPA for the parking space at the Bishop Airport for an initial period of two years with four, one-year options to extend, in an annual amount of \$3,312 payable to the County in monthly installments of \$276 beginning December 1, 2017 and ending November 30, 2019, contingent on the Board’s adoption of future budgets; and authorize the Chairperson to sign, contingent on all appropriate signatures being obtained.
21. **PUBLIC WORKS** – Request Board ratify and approve the Lease Agreement between the County of Inyo and Eastern Sierra Transit Authority, JPA for the terminal building at the Bishop Airport for an initial period of two years with four, one-year options to extend, in an annual amount of \$16,560 payable to the County in monthly installed of \$1,380 beginning December 1, 2017 and ending November 30, 2019, contingent upon the Board’s adoption of future budgets; and authorize the Chairperson to sign, contingent on all appropriate signatures being obtained.
22. **COUNTY ADMINISTRATOR/COUNTY COUNSEL/PUBLIC WORKS** – Request Board consider approving a Credit Rating Agreement with Inyo County Development LLC whereby it will obtain an updated credit rating for the County, the cost of which the County would potentially reimburse in the amount of \$20,000 under terms specified in the Agreement, and authorize the County Administrator to sign.
23. **COUNTY ADMINISTRATOR – Recycling & Waste Management** – Request Board ratify, approve and authorize the Chairperson to sign Amendment No. 1 to the contract between the County of Inyo and Preferred Septic and Disposal, Inc. to start on July 1, 2017 increasing the contract limit payable under the agreement from \$116,496 to \$157,407 and modifying the schedule of fees for the Olancha, Keeler, and Darwin Waste Removal Contract.
24. **COUNTY ADMINISTRATOR – Emergency Services** – Request Board discuss and consider staff’s recommendation regarding continuation of the local emergency known as the “Here It Comes Emergency” that was proclaimed in anticipation of run-off conditions from near-record snowpack posing extreme peril to the safety of property and persons in Inyo County.
25. **COUNTY ADMINISTRATOR – Emergency Services** – Request Board discuss and consider staff’s recommendation regarding continuation of the local emergency known as the “Rocky Road Emergency” that was proclaimed as the result of flooding, mud, and rock landslides and deep snow drifts over portions of Inyo County caused by an atmospheric river weather phenomena that began January 3, 2017 and continued throughout February.
26. **COUNTY ADMINISTRATOR – Emergency Services** – Request Board discuss and consider staff’s recommendation to continue the local emergency known as the “Land of EVEN Less Water Emergency” that was proclaimed as a result of extreme drought conditions that existed until recently in the County, while considering how to address the ongoing hydrologic issues in West Bishop.
27. **COUNTY ADMINISTRATOR – Emergency Services** – Request Board discuss and consider staff’s recommendation regarding continuation of the local emergency known as the “Gully Washer Emergency” that resulted in flooding in the central, south and southeastern portion of Inyo County during the month of July, 2013.
28. **COUNTY ADMINISTRATOR – Emergency Services** – Request Board discuss and consider staff’s recommendation regarding continuation of the local emergency known as the “Death Valley Down But Not Out Emergency” that was proclaimed as a result of flooding in the central, south and southeastern portion of Inyo County during the month of October, 2015.
29. **HEALTH & HUMAN SERVICES – Public Health and Prevention** – Request Board receive a presentation regarding new funding and associated requirements for the tobacco control program and provide direction to staff for development of Tobacco Control Agreement and associated tobacco control plan.

TIMED ITEMS (Items will not be considered before scheduled time but may be considered any time after the scheduled time)

- 1:15 p.m. 30. **COUNTY SERVICES YEAR-IN-REVIEW PRESENTATION** – The County Administrator and County Departments Heads will review departmental highlights in providing public services during 2017. (Presentations will be kept to a strict five-minute limit.)

Note: The agenda items listed below may be considered by the Board at any time during the meeting in the Board's discretion, including before scheduled timed items.

COMMENT (Portion of the Agenda when the Board takes comment from the public and County staff)

31. **PUBLIC COMMENT**

BOARD MEMBER AND STAFF REPORTS



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

For Clerk's Use Only: AGENDA NUMBER 9
--

- Consent Departmental Correspondence Action Public Hearing
 Scheduled Time for Closed Session Informational

FROM: County Administrator

FOR THE BOARD MEETING OF: December 19, 2017

SUBJECT: OKU Solutions

DEPARTMENTAL RECOMMENDATION:

Request your Board approve a purchase order to OKU Solutions in an amount not to exceed \$20,000 for costs associated with cell tower site mapping and related services.

SUMMARY DISCUSSION:

The Fiscal Year 2017-2018 Board Approved Budget includes \$20,000 for a cell tower mapping study to identify optimal sites to locate towers for improving cellular communications in the Owens Valley to improve public safety communications, improve reliability of cell coverage for the public-at-large, and, create a better environment for economic development. Once optimal site locations are identified, the County will embark upon a strategy to acquire those sites, and look at a variety of arrangements – including private sector investment; public investment; and public-private partnerships – to construct the towers and connect them to Digital 395.

Identifying a contractor to perform the mapping proved very challenging. However, with assistance requested from BroadbandUSA during the County's last visit to Washington D.C., David Witkowski of OKU Solutions was identified as capable and willing to perform the study. The County has an agreement in place with OKU Solutions to perform an initial mapping study in an amount not to exceed \$9,950. A copy of the agreement is attached. However, it may be necessary to increase the amount of the agreement, which requires your Board's approval being sought today, in order to evaluate additional sites and for the County to avail itself to related services provided by OKU Solutions.

ALTERNATIVES:

Your Board could choose not to approve the Purchase Order in which case the study will proceed by evaluating a fewer number of potential site locations resulting in a less robust and flexible outcome.


OTHER AGENCY INVOLVEMENT:

Information Services; OKU Solutions

FINANCING:

The Fiscal Year 2017-2018 Economic Development budget includes \$20,000 identified for conducting a cell tower site mapping study.

APPROVALS

COUNTY COUNSEL: N/A	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS <i>(Must be reviewed and approved by county counsel prior to submission to the board clerk.)</i> Approved: _____ Date _____
AUDITOR/CONTROLLER:	ACCOUNTING/FINANCE AND RELATED ITEMS <i>(Must be reviewed and approved by the auditor-controller prior to submission to the board clerk.)</i>  Approved: <u>yes</u> Date <u>12/14/2017</u>
PERSONNEL DIRECTOR: N/A	PERSONNEL AND RELATED ITEMS <i>(Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.)</i> Approved: _____ Date _____

DEPARTMENT HEAD SIGNATURE:

(Not to be signed until all approvals are received)



Date: 12-14-17

County of Inyo – Cellular Site Study

Prepared for: Kevin Carunchio, County of Inyo
Date: 06-Dec-2017

Background

County of Inyo is seeking technical expertise related to creation of a report on suitability of sites within Inyo County for possible cellular network deployments. County staffers will use the report to refine telecommunications planning, apply for grants, and help develop informed responses to build proposals and queries from cellular carriers and site developers will use the site analysis report.

Project Objectives

- Review county-provided GIS data for existing fiber optic lines/conduits, and population mapping.
- Travel to Inyo region for on-site visits and visual site inspections.
- RF coverage studies using Longley-Rice analysis to identify an array of preferred and alternative site locations that would improve cellular coverage in the Owens Valley now and in the future.
- Consider how coverage will benefit schools, population centers, FirstNet public-safety LTE.
- Report authorship, draft review, final report submission

Timeline & Level of Effort

- Commence work ASAP.
- Target on-site visit & site inspection for mid-December.
- LOE Estimate: 8 hours per site (8 bands per site, 1 hour per band setup/run/validate/extract)
- Complete project by Jan 15th 2018.

Scope – Included

- Review of county-provided materials for broadband, conduit, and coverage targets.
- Review (if requested) of CETF or other regional project materials that relate to this project.
- Conversion of USGS mapping data to EDX Signal format.
- RF coverage studies for selected wireless sites. Studies for each site will focus on the primary voice band and primary data band for the four major U.S. cellular carriers (Verizon, AT&T, Sprint, T-Mobile).
- Travel to Inyo County for on-site and visual inspections.
- Report authorship and editing.

Scope – Excluded

- RF coverage analysis software. (County to purchase, Oku will use and return to County.)
- Based on successful outcomes of this project, and mutual agreement to continue, we are pleased to consider additional projects excluded from the scope of this project:
 - Ray-tracing studies (effect of buildings on coverage in urban environments).
 - Indoor coverage studies.
 - Public safety wireless (NBFM, P25, etc.) systems.
 - Coverage studies for additional data bands and/or carriers.
 - Acting as an advisor in discussions with, or reviewing proposals from, wireless carriers and site developers.
 - Assisting with FirstNet planning or discussions.
 - Authoring of grant proposals.
 - On-site RF spectrum analysis, spectrum clearing, or interference analysis.
 - On-site passive intermodulation analysis.

Deliverables

- Regular progress updates via email or phone.
- Expert report detailing the pros and cons of various locations for wireless siting.

Major Milestones

- Commencement – (County delivers initial materials to Oku Solutions).
- Initial material review – (Oku Solutions, followed by joint progress teleconf).
- Travel to Inyo County – (Oku Solutions, mid-December).
- RF coverage studies – (Oku Solutions).
- Draft report authorship – (Oku Solutions, followed by review teleconf).
- Report revision, final authorship – (Oku Solutions).

Change Control

- Changes to this project must be reviewed by both County of Inyo's designated representative and Oku Solutions. Changes must be acknowledged and approved by all stakeholders. Approval via email is OK.

Reporting and Communications

- Bi-weekly 30 minute teleconference.
- Emails and additional teleconferences as needed and agreed.

Project Costs

- Rate: Government/Preferred rate.
- Total cost: \$9,950
- Included
 - Consultant expertise.
 - Consultant travel time, airfare, lodging.
- Excluded
 - Required software licensing.
- Presumptions: County of Inyo will purchase RF propagation software per specification by Oku Solutions. County of Inyo will retain ownership and licensing for this software after project is completed.

Payment Terms

- 50% prior to commencement of work.
- 50% on completion of final draft.

If the terms and descriptions enumerated here meet your satisfaction, we ask you to sign below and return a signed copy to Oku Solutions. This signed document will serve as our contract and Notice to Proceed. We will invoice only upon receipt of the Notice to Proceed.

Notice to Proceed:


Kevin Carunchio, County Administrator, County of Inyo

12-07-2017

Approved/Submitted
David T. Witkowski
Oku Solutions LLC
8-DEC-2017



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

For Clerk's Use Only:
AGENDA NUMBER
 10

- Consent
 Departmental
 Correspondence Action
 Public Hearing
 Scheduled Time for
 Closed Session
 Informational

FROM: Information Services

FOR THE BOARD MEETING: December 19, 2017

SUBJECT: Local Update of Census Addresses Operation

DEPARTMENTAL RECOMMENDATION:

Request Board approve Inyo County participation in the Local Update of Census Addresses (LUCA) Operation in support of the U.S. Census Bureau's decennial census of 2020.

SUMMARY DISCUSSION:

LUCA is the only opportunity offered to local, state, and tribal governments to review and comment on the U.S. Census Bureau's residential address list for their jurisdiction prior to the 2020 Census. The Census Bureau relies on a complete and accurate address list to reach every living quarters and associated population for inclusion in the census. The Census Address List Improvement Act of 1994 (Public Law 103-430) authorizes the LUCA. Governments that participate in LUCA help ensure an accurate decennial census count for their communities. An accurate count helps the federal government annually allocate more than \$675 billion across 26 federal agencies for local, state, and tribal government programs and services.

ALTERNATIVES:

Decline approval.

OTHER AGENCY INVOLVEMENT:

Planning Department.

FINANCING: N/A

<u>APPROVALS</u>	
COUNTY COUNSEL: N/A	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS <i>(Must be reviewed and approved by county counsel prior to submission to the board clerk.)</i> Approved: _____ Date _____
AUDITOR/CONTROLLER: N/A	ACCOUNTING/FINANCE AND RELATED ITEMS <i>(Must be reviewed and approved by the auditor-controller prior to submission to the board clerk.)</i> Approved: _____ Date _____
PERSONNEL DIRECTOR: N/A	PERSONNEL AND RELATED ITEMS <i>(Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.)</i> Approved: _____ Date _____

DEPARTMENT HEAD SIGNATURE:
 (Not to be signed until all approvals are received)

Date: Dec 12, 2017



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

- Consent
 Departmental
 Correspondence Action
 Public Hearing
 Schedule time for
 Closed Session
 Informational

For Clerk's Use Only:
AGENDA NUMBER
11

FROM: Public Works Department
 FOR THE BOARD MEETING OF: December 19, 2017
 SUBJECT: Resolution and Notice of Completion for the Water Department Roof Sealing Project

DEPARTMENTAL RECOMMENDATIONS:

1. Recommend your Board approve the resolution accepting the improvements for the Water Department Roof Sealing Project; and,
2. Authorize the recording of a Notice of Completion for the Water Department Roof Sealing Project (Project).

CAO RECOMMENDATION:

SUMMARY DISCUSSION: This Project was included in the 16/17 Deferred Maintenance List, and was carried over into the 17/18 budget. On September 19th, 2017 the County awarded the job to Universal Coatings, Inc. of Fresno, CA for a price of \$28,250.00.


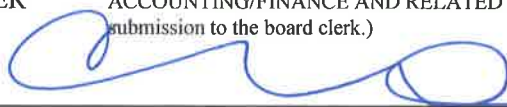
On November 17, 2017 the final inspection was performed and the installation was determined to be complete to the satisfaction of the Public Works Director. Accordingly, the Director is requesting that the Board adopt the attached Resolution, which accepts the completed improvements and authorizes the Public Works Director to record a Notice of Completion for the project.

ALTERNATIVES: The Board could choose not to approve the resolution. Consequently, the project would not be formally accepted and the Notice of Completion could not be filed. This is not recommended, because the work was satisfactorily completed.

OTHER AGENCY INVOLVEMENT: County Counsel has reviewed the resolution.

FINANCING: The cost of the roof sealing was funded through budget unit 011501 16/17 Deferred Maintenance Budget, object code 5191.

APPROVALS

COUNTY COUNSEL:	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS (Must be reviewed and approved by County Counsel prior to submission to the board clerk.)
	Approved: <u>yes</u> Date <u>11/30/17</u>
AUDITOR/CONTROLLER	ACCOUNTING/FINANCE AND RELATED ITEMS (Must be reviewed and approved by the auditor/controller prior to submission to the board clerk.)
	Approved: <u>eps</u> Date <u>12/4/2017</u>
PERSONNEL DIRECTOR	PERSONNEL AND RELATED ITEMS (Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.)
	Approved: _____ Date _____

DEPARTMENT HEAD SIGNATURE:  Date: 12/7/17
 (Not to be signed until all approvals are received)

RESOLUTION #2017 - ____

**A RESOLUTION OF THE BOARD OF SUPERVISORS
OF THE
COUNTY OF INYO, STATE OF CALIFORNIA
AUTHORIZING THE RECORDING OF A NOTICE OF COMPLETION
FOR THE
WATER DEPARTMENT ROOF SEALING PROJECT**

WHEREAS, Clint Quilter, Director of the Public Works Department of the County of Inyo, has determined that the Water Department Roof Sealing Project has been completed by Universal Coatings, Inc. in accordance with the project quote details.

NOW, THEREFORE, BE IT RESOLVED, that the Director of Public Works is hereby authorized and directed to sign and file with the County Recorder a separate Notice of Completion pertaining to the Water Department Roof Sealing Project.

Passed, approved and adopted this _____ day of _____, 2017 by the following vote:

AYES:

NOES:

ABSENT:

ABSTAIN:

Chairperson, Board of Supervisors

ATTEST:

Kevin Carunchio, Clerk

by _____
Assistant Clerk of the Board

**RECORDING REQUESTED BY AND
WHEN RECORDED RETURN TO:**

**Inyo County Public Works Department
P. O. Drawer Q
Independence, CA 93515**

The area above this line is for Recorder's Use

NOTICE OF COMPLETION

NOTICE IS HEREBY GIVEN THAT:

1. A work of improvement known as the Water Department Roof Sealing Project on the property hereinafter described was completed on November 17, 2017 and was accepted by the Inyo County Board of Supervisors on _____.
2. The property on which the Water Department Roof Sealing Project has been completed is located at 135 S. Jackson St, Independence, CA.
3. The County of Inyo, a political subdivision of the State of California, the address of which is 224 North Edwards Street, P.O. Drawer N, Independence, CA 93526, owns and maintains the Water Department building.
4. The undersigned Clint Quilter is the Director of Public Works of the County of Inyo and has been duly authorized pursuant to Resolution adopted November 10, 2015, by the Board of Supervisors of the County of Inyo to execute and file this Notice of Completion.
5. The name of the original contractor that constructed the Water Department Roof Sealing Project pursuant to the purchase order with the owner is Universal Coatings, Inc. of Fresno, California.

Pursuant to the purchase order, the contractor was required to furnish all labor, materials, methods or processes, implements, tools, machinery, equipment, transportation services, and all other items and related functions that are necessary or appurtenant to construct the project designated in the purchase order.

COUNTY OF INYO

Dated: _____

By: _____
Clint Quilter, Director of Public Works



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

- Consent
 Departmental
 Correspondence Action
 Public Hearing
 Schedule time for
 Closed Session
 Informational

For Clerk's Use Only:
AGENDA NUMBER 12

FROM: Public Works Department

FOR THE BOARD MEETING OF: December 19, 2017

SUBJECT: Approve Amendment #2, extending the contract term and leaving the current payments of \$18,136 per month to the amount with Wilder Barton for the operation and maintenance of the Independence, Lone Pine and Laws Town Water Systems.

DEPARTMENTAL RECOMMENDATIONS:

1. Approve Amendment #2 to the current Standard Contract #116 with Wilder Barton for the operation and maintenance of the Independence, Laws and Lone Pine town water systems, extending the term through December 31, 2018 unless terminated earlier; and increasing total contract amount not to exceed \$924,300.
2. Authorize the Chairperson to sign the Amendment to the Contract contingent upon the appropriate signatures being obtained and contingent upon the adoption of future budgets.

CAO RECOMMENDATION:

SUMMARY DISCUSSION:

Inyo County first entered into an agreement with Wilder Barton Inc. to provide operations and maintenance services for the Lone Pine, Independence and Laws water distribution systems on July 1, 2014. The current amendment #1 extending the contract with Wilder Barton Inc. will come to an end on December 29, 2017. The request for an additional one year extension is to provide staff more time to evaluate possible proposals and/or negotiate a contract for a possible longer term agreement for the operations and maintenance of the water systems.

ALTERNATIVES:

Your Board could deny the amendment to this contract and direct the Public Works Department to operate and maintain the system using county forces, however, that is not recommended as the Public Works Department does not have sufficient staffing or appropriate certificates at the current time to accomplish it.

OTHER AGENCY INVOLVEMENT:

County Counsel
Auditor

FINANCING:

Financing for this contract is included in the Preliminary and Proposed 2017-2018 budgets for the Lone Pine, Independence, and Laws Water Systems (152101, 152201 and 152301), object code 5265, Professional and Special Services.

APPROVALS

COUNTY COUNSEL: AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS (Must be reviewed and approved by County Counsel prior to submission to the board clerk.)

[Handwritten Signature]

Approved: YES Date 12/5/17

AUDITOR/CONTROLLER ACCOUNTING/FINANCE AND RELATED ITEMS (Must be reviewed and approved by the auditor/controller prior to submission to the board clerk.)

[Handwritten Signature]

Approved: YES Date 12/6/17

PERSONNEL DIRECTOR PERSONNEL AND RELATED ITEMS (Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.)

Approved: _____ Date _____

DEPARTMENT HEAD SIGNATURE:
(Not to be signed until all approvals are received)

[Handwritten Signature]

Date: 12/8/17

**AMENDMENT NUMBER 2 TO
AGREEMENT BETWEEN THE COUNTY OF INYO AND
WILDER BARTON, INC.
FOR THE PROVISION OF INDEPENDENT CONTRACTOR SERVICES**

WHEREAS, the County of Inyo (hereinafter referred to as "County") and
WILDER BARTON, INC., of BISHOP, CA
(hereinafter referred to as "Contractor"), have entered into an Agreement for the Provision of Independent
Contractor Services dated JULY 1, 2014, on County of Inyo Standard
Contract No. 116, for the term from JULY 1, 2014 to JUNE 30, 2017.

WHEREAS, County and Contractor do desire and consent to amend such Agreement as set forth
below;

WHEREAS, such Agreement provides that it may be modified, amended, changed, added to, or
subtracted from, by the mutual consent of the parties thereto, if such amendment or change is in written
form, and executed with the same formalities as such Agreement, and attached to the original Agreement
to maintain continuity.

County and Contractor hereby amend such Agreement as follows:

Amend Section 2 TERM, to read as follows;

2. TERM

The term of the agreement shall be extended for a period of one year from January 1, 2018 thru December 31, 2018 unless
terminated as provided below.

Amend Section 3.D Limit upon the amount payable under the Agreement. The total sum of all payments made by the County to
the contractor for the services and work performed under this Agreement shall not exceed \$924,300.

The effective date of this Amendment to the Agreement is January 1, 2018.

All the other terms and conditions of the Agreement are unchanged and remain the same.

AMENDMENT NUMBER 2 TO
AGREEMENT BETWEEN THE COUNTY OF INYO AND
WILDER BARTON, INC.
FOR THE PROVISION OF INDEPENDENT CONTRACTOR SERVICES

IN WITNESS THEREOF, THE PARTIES HERETO HAVE SET THEIR HANDS AND SEALS THIS
____ DAY OF _____, _____.

COUNTY OF INYO

By: _____

Dated: _____

CONTRACTOR

By: _____

Signature

Type or Print

Dated: _____

APPROVED AS TO FORM AND LEGALITY:

County Counsel

APPROVED AS TO ACCOUNTING FORM:

County Auditor

APPROVED AS TO PERSONNEL REQUIREMENTS:

Personnel Services

APPROVED AS TO RISK ASSESSMENT:

County Risk Manager



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

- Consent Departmental Correspondence Action Public Hearing
- Schedule time for Closed Session Informational

For Clerk's Use Only:
AGENDA NUMBER
13

FROM: Auditor-Controller

FOR THE BOARD MEETING OF: December 19, 2017

SUBJECT: Second Review of the Social Security Number Truncation Program

DEPARTMENTAL RECOMMENDATIONS: Approve the Second Review of the Social Security Number Truncation Program report prepared by the Auditor's Office

CAO RECOMMENDATION:

SUMMARY DISCUSSION: AB 1168 was signed into law by the Governor on October 13, 2007. The law intended to protect against identity theft by requiring local agencies to redact social security numbers from records prior to disclosing them to the public. The law authorized the County to establish an additional \$1 fee for the first page of each recorded document to fund implementation of the program.

County Recorders were required to establish social security truncation programs in order to create a public record version of every official record that contains a social security number. The public record version is an exact copy of the official record but with any social security number showing no more than the last four digits. The provision applies to all documents recorded since 1980.

The Board of Supervisors authorized the fee on December 11, 2007 with Resolution No. 2007-56

Authorization of the fee requires that the County Auditor conduct two reviews to verify the funds generated by the fee are used only for the purpose of the program and to conduct the reviews. The first review must be completed between June 1, 2012 and December 31, 2013. The second review must be completed between June 1, 2017 and December 31, 2017. The reviews must state the progress of the County Recorder in truncating recorded documents pursuant to subdivision (a) of Government Code Section 27301, and be available to the public.

The fee will sunset after December 31, 2017, unless it has been reauthorized by the Board. If outside funding is obtained to implement the program, the fee may be charged until the debt is repaid. No outside funding was borrowed to implement the program and the annual fee for the software is \$900.00. Fees collected as of 6/30/2017 are \$35,620.50. The cost of the program, as of 6/30/2017 has been \$37,372.60. The difference between collections and costs is \$1752.10.

The review found that the Social Security Number Truncation Program is working correctly and all records since 1980 have been truncated.

ALTERNATIVES: The Board could choose to not approve the report.

OTHER AGENCY INVOLVEMENT: County Clerk

FINANCING:

APPROVALS

COUNTY COUNSEL:	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS (Must be reviewed and approved by County Counsel prior to submission to the board clerk.)	Approved: <u>YES</u>	Date <u>12/1/17</u>
AUDITOR/CONTROLLER	ACCOUNTING/FINANCE AND RELATED ITEMS (Must be reviewed and approved by the auditor/controller prior to submission to the board clerk.)	Approved: <u>YES</u>	Date <u>11/29/17</u>
PERSONNEL DIRECTOR	PERSONNEL AND RELATED ITEMS (Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.)	Approved: _____	Date _____

DEPARTMENT HEAD SIGNATURE:

(Not to be signed until all approvals are received)

Chy Shepherd

Date: 11/29/17



**COUNTY OF INYO
OFFICE OF THE AUDITOR-CONTROLLER**

P. O. Drawer R
Independence, California 93526

**Review of the Social Security Number Truncation Program
Review Period July 1, 2013 through June 30, 2017**

Prepared by the Office of the Inyo County Auditor
December 2017

Background:

AB 1168 was signed into law by the Governor on October 13, 2007. The law intends to protect against identity theft by requiring local agencies to redact social security numbers from records prior to disclosing them to the public. The law authorized the County to establish an additional \$1.00 fee for the first page of each recorded document to fund implementation of the program.

County Recorders were required to establish social security truncation programs in order to create a public record version of every official record that contains a social security number. The public record version is an exact copy of the official record but without any social security number showing more than the last four digits. The provision applies to all documents recorded since 1980.

The Board of Supervisors authorized the \$1.00 fee on December 11, 2007 with Resolution No. 2007-56

Authorization of the fee requires that the County Auditor conduct two reviews to verify the funds generated by the fee are used only for the purpose of the program and to conduct the reviews. The first review was completed between June 1, 2012 and December 31, 2013. The second review must be completed between June 1, 2017 and December 31, 2017. The reviews must state the progress of the County Recorder in truncating recorded documents pursuant to subdivision (a)

of Government Code Section 27301, and making the review available to the public.

The fee will sunset after December 31, 2017, unless it has been reauthorized by the Board. If outside funding is obtained to implement the program, the fee may be charged until the debt is repaid.

Review Period:

July 1, 2013 to June 30, 2017

Analysis and Estimates:

The Clerk-Recorder estimated that the back file of documents from 1996-to May 30, 2008 was 215,500 and that the office would create 12,000 images a year from that date forward. The estimated cost to truncate the back file of 215,500 images and for the first year of operation was \$17,873.00. The Board of Supervisors authorized the purchase of the AtPac truncation/redaction system at its January 6, 2009 meeting.

It was anticipated, in 2009, that the ongoing cost to redact a document would be \$.06 per image for an annual cost of \$720.00

Progress of County Recorder in Truncating Recorded Documents pursuant to subdivision (a) of Government Code Section 27301:

All the records from 1980 to 1995 have been converted to a digital format. The Clerk's office has installed additional software, ID Shield from AtPac, to complete the social security redaction process for all records from 1980 to date

The initial audit revealed that all records from 1980 to 1994 had been redacted correctly but that the records from 1995 had not. Corrective measures were implemented and the 1995 records have been redacted.

A random audit of records from 1995 through June 30, 2017 found all records have been truncated and the program is operating correctly.

Fiscal Analysis:

Redaction Fees were collected beginning January 2, 2008. The total amount collected as of June 30, 2017 is \$35,620.50

FY2007/2008:	\$1,916.00
FY2008/2009:	\$3,567.00
FY2009/2010:	\$3,504.00
FY2010/2011:	\$3,651.00
FY2011/2012:	\$3,557.00
FY2012/2013:	\$4,572.50
FY2013/2014	\$3,271.00
FY2014/2015	\$3,409.00
FY2015/2016	\$3,246.00
FY2016/2017	\$5,017.00

Expenditures to implement the program through June 30, 2017 have totaled \$37,372.60. The difference between collections and costs is \$1,752.10.

The first audit showed the true cost at \$.09 per page, but predicted that the cost per page would decline because the initial expenses to digitize old records had already occurred and new records are already digitized and truncated by the software when they are created. The current annual fee for the truncation software is \$900.00 and at an average of 12,000 pages a year this is a cost of \$.075 per page.

Summary:

The Social Security Number Truncation Program has been implemented correctly and all records from 1980 to date have been truncated. The cost per page is declining to \$0.075 a page and the annual costs are \$900.00. The \$35,620.50 in fees collected has been used to offset the \$37,372.60 expenses of the program. All fees collected have been used exclusively to implement the program. The \$1.00 fee that was adopted by the Board of Supervisors on December 11, 2007 will expire on 12/31/2017.



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

For Clerk's Use Only:
AGENDA NUMBER

14

- Consent Departmental Correspondence Action Public Hearing
 Scheduled Time for Closed Session Informational

FROM: Kammi Foote, Clerk-Recorder and Registrar of Voters

FOR THE BOARD MEETING OF: December 19, 2017

SUBJECT: Authorization to purchase of new Voting System

DEPARTMENTAL RECOMMENDATION:

Request that the Board of Supervisors:

- A) Authorize the Clerk-Recorder to enter into a contract for the provisions of a New Voting System in an amount not to exceed \$201,796 plus shipping for the period of the Agreement effective date through December 31, 2025; and
- B) Declare Dominion Voting Systems, Inc the sole source provider for a New Voting System and Managed Services related to the New Voting System; and
- C) Amend the Fiscal Year 2017-2018 Election Innovation (Budget 500202) as follows: increase appropriation in Equipment (Object Code 5650) by \$211,796 (4/5th vote required).

SUMMARY DISCUSSION:

The current voting system was purchased from Sequoia Voting Systems in 2005 after the previous punch-card system was decertified in response to national concerns raised during the 2000 Presidential election. The funding for that purchase – approximately \$700,000 -- derived from a combination of the Help America Vote Act (HAVA), California's voter approved Proposition 41 and matching General Fund monies.

In 2007, Secretary of State Debra Bowen decertified, and then conditionally recertified, the hardware and software of the Sequoia voting system. At present, Inyo County still uses this voting system (now owned by Dominion Voting). Most Inyo County citizens vote on a paper ballot that is tabulated with an Optech scanner at the Central Count Location in Independence. In addition, each voting location is supplied with one federally mandated accessible Edge II touch screen voting machine.

Due to the increasing unreliability of the County's aging voting equipment, and changes in technology and voting laws, it was recommended that the County develop a plan for replacing the voting system before the 2018 election.

On June 1, 2017 an RFP was issued for a New Voting System. The County received four responsive proposals.

On October 3, 2017, the Inyo County Board of Supervisors declared Dominion Voting Systems as the successful bidder for the lease or purchase of a New Voting System. The Board also authorized the Clerk-Recorder to enter into further negotiations with Dominion Voting System for the purchase or lease of a New Voting System.

After conferring with the County Administrator and the County Auditor, the Clerk-Recorder and vendor drafted the attached contract for an outright purchase of the New Voting System, with an eight year service agreement that includes an of adjudication station, client workstation and server during the term of the agreement.

ALTERNATIVES:

The Board can deny authorization of this Agreement and associated payment.

FINANCING:

There is currently \$216,869.97 in the Elections Innovation Fund, which is sufficient to cover the outright purchase of the New Voting System. In addition to the purchase of the voting equipment, there is an On-going annual software license and hardware warranty cost of approximately \$13,500 that will have to be budgeted in future budgets, as part of this agreement. The annual software license fee of \$9,350 is subject to a 5% annual adjustment. This is a reduction from our current annual license fee of \$11,008.61 FY 2016/2017 – which was also subject to a 5% annual adjustment.

APPROVALS	
COUNTY COUNSEL:	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS (Must be reviewed and approved by County Counsel prior to submission to the Board Clerk.) Approved:  Date: 11/29/2017
AUDITOR/CONTROLLER:	ACCOUNTING/FINANCE AND RELATED ITEMS (Must be reviewed and approved by the Auditor/Controller prior to submission to the Board Clerk.)  Approved:  Date: 11/30/2017
PERSONNEL DIRECTOR:	PERSONNEL AND RELATED ITEMS (Must be reviewed and approved by the Director of Personnel Services prior to submission to the Board Clerk.) Approved: _____ Date: _____
BUDGET OFFICER:	BUDGET AND RELATED ITEMS (Must be reviewed and approved by the Budget Officer prior to submission to the Board Clerk.)  Approved:  Date: 12-01-2017

DEPARTMENT HEAD SIGNATURE:

(Not to be signed until all approvals are received)



Date: 12/4/2017

VOTING SYSTEM AGREEMENT
BY AND BETWEEN
DOMINION VOTING SYSTEMS, INC.
AND INYO COUNTY, CA

This Voting Systems Agreement (the "Agreement"), dated the 13th day of October, (the "Effective Date"), for a voting system services, software licenses and related services is made by and between Inyo County, CA having its principal office located at 1400 W Lacey Blvd., Hanford, CA 93230 (hereinafter the "Customer"), and Dominion Voting Systems Inc., having its principal office located at 1201 18th Street, Suite 210, Denver, CO 80202 (hereinafter "Dominion"). This Agreement may refer to Dominion and the Customer together as the "Parties," or may refer to Dominion or the Customer individually as a "Party."

WHEREAS, the Customer desires to purchase voting system services, and software use licenses; and

WHEREAS, Dominion designs, manufactures, licenses, and provides services for its voting systems.

NOW THEREFORE, in consideration of the mutual covenants contained herein, and in accordance with the terms and conditions set forth herein, Dominion agrees to license and furnish the System (as defined herein) to the Customer.

1. **Composition of Agreement.** Exhibits A and B are attached and incorporated herein by reference and form a part of this Agreement. This Agreement consists of the terms and conditions contained in the following sections and the listed Exhibits. The total compensation payable under this Agreement shall be in accordance with the item prices incorporated within the Exhibit A attached hereto (Pricing Summary and Deliverables Description) and all other services related to the performance of this Agreement.

Exhibit A: Pricing Summary and Deliverables Description
Exhibit B: Software License Terms and Conditions

2. **Definitions.** For the purposes of this Agreement, the following are defined terms:

- 2.1. "Acceptance" and variations thereof, means the successful completion by the Customer of the acceptance testing performed on each component of Dominion Hardware and Software, after delivery in accordance with testing criteria developed and agreed to by the parties, or the occurrence of other events defined in Section 8.

- 2.2. "Confidential Information" means those materials, documents, data, and technical information, specifications, business information, customer information, or other information of a Party (the "Disclosing Party") maintains as trade secrets or confidential and which are disclosed to a another Party (the "Receiving Party") in tangible form conspicuously marked as "confidential," or with words having similar meaning, which includes without limitation, Dominion Software and associated documentation.

- 2.3. "Dominion Hardware" means the ImageCast[®] system hardware as more specifically described in Exhibit A.
 - 2.4. "Dominion Software" means software and firmware programs licensed to the Customer by Dominion and any associated documentation including the following:
 - 2.5. "Election" means a single election event administered by the Customer including any absentee and early voting activity associated with the election event. Election shall not mean any follow-on events occurring after the initial election event, including without limitations, run-offs or recall replacements elections. Any follow on event shall be considered an Election in and of itself.
 - 2.6. "Election Management System Hardware" or "EMS Hardware" means third party hardware required for operating Dominion Software as used in conjunction with the Dominion Hardware.
 - 2.7. "License" has the meaning set forth in Section 7.
 - 2.8. "System" means the combination of Dominion Software, Dominion Hardware and EMS Hardware.
 - 2.9. "Third Party Software" means manufacturer supplied software, or firmware owned by third parties, which Dominion provides to Customer pursuant to sublicenses or end user license agreements with the owners of such Third Party Software. Third Party Software includes, but is not limited to, various operating systems, software drivers, report writing subroutines, and firmware.
3. **Term of Agreement.** The Term of this Agreement shall begin on the Effective Date and shall continue until December 31, 2025, unless sooner terminated or extended as provided herein.
4. **Dominion's Responsibilities.** Dominion shall:
- 4.1. Deliver the System and services as described in Exhibit A - Pricing and Payment Summary and Deliverables Description.
 - 4.2. Provide the Customer with a Dominion Software use License as described in Exhibit B - Software License Terms.
 - 4.3. Assign a Dominion project manager ("Dominion Project Manager") to oversee the general operations of the project. The Dominion Project Manager will be the primary contact for all project needs. The Dominion Project Manager will be responsible for all deliverables and services including, resource planning and coordination, product delivery, issue resolution and for all administrative matters such as invoices and payments.

- 4.4. Assist in the Acceptance testing process as required by Section 8 herein.
- 4.5. Provide Customer with one (1) reproducible electronic copy of the documentation.
- 4.6. Provide invoices to Customer pursuant to the payment schedule in Exhibit A and the payment terms described in Section 5.1 herein.

5. Customer's Responsibilities. Customer shall:

- 5.1. Pay invoices in a timely manner and no later than thirty (30) calendar days from receipt of a Dominion invoice.
 - 5.1.1. Dominion shall issue invoices to Customer pursuant to the invoice schedule listed in Exhibit A.
 - 5.1.2. Payments specified in this Section 5 are exclusive of all excise, sale, use and other taxes imposed by any governmental authority, all of which shall be reimbursed by the Customer. If the Customer is exempt from taxes, Customer shall supply Dominion a tax exemption certificate or other similar form demonstrating its exempt status.
- 5.2. Assign a Customer project manager ("Customer Project Manager"), who shall be responsible for review, analysis and acceptance of the System and the coordination of Customer personnel, equipment, vehicles and facilities. The Customer Project Manager shall be empowered to make decisions on behalf of the Customer with respect to the work being performed under this Agreement. The Customer Project Manager shall also have direct access to the Customer's top management at all times for purposes of problem resolution.
- 5.3. Conduct Acceptance testing process as required by Section 8.
- 5.4. Customer shall provide reasonable access and entry into all Customer property required by Dominion to perform the services described in this Agreement. All such access and entry shall be provided at Customer's expense.
- 5.5. When applicable, for election setup and database creation services as described in Exhibit A, the Customer shall review and approve or identify issues to all Dominion deliverables related to such service within two (2) business days of receipt by the Customer. In the event the Customer discovers an issue, it shall provide written notice to Dominion immediately following the discovery of any issue and Dominion shall rectify the issue at no additional cost to the Customer. In the event the Customer approves the deliverable and subsequent to such approval, request that a change be made to the deliverable, then Dominion may provide the change at an additional cost based upon Dominion's then current published service rates.

6. Title and Risk of Loss.

- 6.1. Title to the System, Excluding All Software. Title to the System, or any portion thereof, excluding software and firmware, will pass to Customer upon delivery.
- 6.2. Software. Software, including firmware, is licensed not sold. The original and any copies of the Dominion Software, or other software provided pursuant to this agreement, in whole or in part, including any subsequent improvements or updates, shall remain the property of Dominion, or any third party that owns such software.
- 6.3. Risk of Loss. Dominion shall bear the responsibility for all risk of physical loss or damage to each portion of the System until such portion is Accepted by Customer. Customer shall provide Dominion with a single location for shipment and Dominion shall not be responsible for shipping to more than one location. To retain the benefit of this clause, Customer shall notify Dominion of any loss or damage within ten (10) business days of the receipt of any or all portions of the System, or such shorter period as may be required to comply with the claims requirements of the shipper, and shall cooperate in the processing of any claims made by Dominion.

7. Software License and Use.

- 7.1. License. Upon mutual execution of this Agreement, Dominion grants to the Customer, and the Customer accepts a non-exclusive, non-transferable, license ("License") to use the Dominion Software subject to the terms and conditions of this Agreement and the Software License Terms attached hereto as Exhibit B.
- 7.2. Third Party Software. The System includes Third Party Software, the use of which is subject to the terms and conditions imposed by the owners of such Third Party Software. Customer consents to the terms and conditions of the third party License Agreements by Customer's first use of the System.

8. Acceptance.

- 8.1. Dominion Software or Dominion Hardware Testing. After delivery of Dominion Software or Dominion Hardware, the Customer will conduct Acceptance testing of such units, in accordance with the Acceptance criteria developed and updated, from time to time, by Dominion. Such Acceptance testing shall occur at a time mutually agreed upon by the Parties, but no later than ten (10) business days after installation.
- 8.2. System Acceptance Testing. To the extent not tested as part of the testing pursuant to Subsections 8.1, upon completing the installation of the System, the Customer will conduct system acceptance testing, according to the Acceptance test procedures developed and updated, from time to time, by Dominion. Such Acceptance testing shall occur at a time mutually agreed upon by the Parties, but no later than ten (10) business days after installation of the System.

- 8.3. Acceptance/Rejection. After testing, if the Dominion Software, Dominion Hardware, or the System does not conform to user documentation or Dominion provided Acceptance criteria, Customer will notify Dominion in writing within five (5) business days. Dominion will, at its own expense, repair or replace the rejected Dominion Software, Dominion Hardware, or System within thirty (30) days after receipt of Customer's notice of deficiency. The foregoing procedure will be repeated until Customer finally accepts or rejects the Dominion Software, Dominion Hardware, or System in writing in its sole discretion.
- 8.4 System Conformance. Customer will not refuse to grant Acceptance of the System, in whole or in part, solely for the reason that it fails to conform with the specifications, requirements and functions set out in the Agreement in a manner that does not affect the performance of the System, in whole or in part, and Dominion shall provide a plan of action to cure such non-conformity with reasonable dispatch.

9. Warranties.

- 9.1. Dominion Software Warranty. The Dominion Software warranty is subject to the terms and conditions of Exhibit B - the Software License Terms.
- 9.2. Third Party Products. The warranties in this Sections 9 do not apply to any third party products. However, to the extent permitted by the manufacturers of third party products, Dominion shall pass through to Customer all warranties such manufacturers make to Dominion regarding the operation of third party products.
- 9.3. Dominion Hardware Warranty Terms. Dominion warrants that when used with the hardware and software configuration purchased through or approved by Dominion, each component of Dominion Hardware will be free of defects that would prevent the Dominion Hardware from operating in conformity in all material respects with its specifications as documented by Dominion. The Dominion Hardware Warranty shall remain in effect during the Agreement Term.
- 9.4. Dominion Hardware Warranty Services. If any Dominion Hardware component fails to operate in conformity with its specifications during the warranty period, Dominion shall provide a replacement for the Dominion Hardware component or, at Dominion's sole option, shall repair the Dominion Hardware component, so long as the Dominion Hardware is operated with its designated Dominion Software and with third party products approved by Dominion for use with the Dominion Hardware. The following conditions apply to the Dominion Hardware warranty:
- 9.4.1. Dominion shall perform one (1) on-site preventative maintenance inspection ("PM") per year on Dominion Hardware during the Agreement Term at a time mutually agreed to by the Parties. This on-site PM is expected to be scheduled at least ninety (90) days prior to requested test date. Dominion shall perform the annual PM and will replace any and all parts

that fail due to normal use during the warranty period. In the event of a warranty claim outside of the scheduled PM, additional on-site service will be available at Dominion's then current time and material rates. There are no additional charges for parts covered by this warranty.

9.4.2. The following services are not covered by this Agreement, but may be available at Dominion's current time and material rates:

9.4.2.1. Replacement of consumable items including but not limited to batteries, paper rolls, ribbons, seals, smart cards, and removable memory devices, scanner rollers, disks, etc.;

9.4.2.2. Repair or replacement of Dominion Hardware damaged by of accident, disaster, theft, vandalism, neglect, abuse, or any improper usage;

9.4.2.3. Repair or replacement of Dominion Hardware modified by any person other than those authorized in writing by Dominion;

9.4.2.4. Repair or replacement of Dominion Hardware from which the serial numbers have been removed, defaced or changed.

9.5. No Other Warranties. DOMINION DISCLAIMS ALL OTHER WARRANTIES, AND REPRESENTATIONS, WHETHER WRITTEN, ORAL, EXPRESS, IMPLIED OR STATUTORY, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY BASED ON A COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE.

10. Force Majeure. Should any circumstances beyond the control of Dominion or Customer occur that delay or render impossible the performance of any obligation due under this Agreement, such obligation will be postponed for the period of any delay resulting from any such circumstances, plus a reasonable period to accommodate adjustment to such extension, or cancelled if performance has been rendered impossible thereby. Such events may include, without limitation, accidents; war, acts of terrorism; natural disasters; labor disputes; acts, laws, rules or regulations of any government or government agency; or other events beyond the control of both Dominion and Customer. Neither Party shall be liable under this Agreement for any loss or damage to the other Party due to such delay or performance failures. Notwithstanding the foregoing, both Parties shall use their commercially reasonable efforts to minimize the adverse consequences of any such circumstances. This Section shall not operate to excuse any Party from paying amounts that are owed pursuant to this Agreement.

11. Indemnification. Dominion, at its sole expense, will indemnify and defend the Customer, its officers, agents and employees from and against any loss, cost, expense or liability (including but not limited to attorney's fees and awarded damages) arising out of a claim, suit or action that the System infringes, violates, or misappropriates a Third Party's patent, copyright, trademark, trade secret or other intellectual property or proprietary rights.

12. Limitation of Liability. EXCEPT FOR THE INDEMNIFICATION OBLIGATIONS CONTAINED IN THIS AGREEMENT, DOMINION'S TOTAL AGGREGATE LIABILITY FOR ANY LOSS, DAMAGE, COSTS OR EXPENSES UNDER OR IN CONNECTION WITH THIS AGREEMENT, HOWSOEVER ARISING, INCLUDING WITHOUT LIMITATION, LOSS, DAMAGE, COSTS OR EXPENSES CAUSED BY BREACH OF CONTRACT, NEGLIGENCE, STRICT LIABILITY, BREACH OF STATUTORY OR ANY OTHER DUTY SHALL IN NO CIRCUMSTANCES EXCEED THE TOTAL DOLLAR AMOUNT OF THE AGREEMENT. NEITHER PARTY SHALL BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF DATA, LOSS OF USE OR ANY OTHER INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL LOSS OR DAMAGE WHATSOEVER, HOWSOEVER ARISING, INCURRED BY THE OTHER PARTY OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT, NEGLIGENCE OR OTHER TORT, EVEN IF THE PARTIES OR THEIR REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

13. Confidential Information.

- 13.1. Each Party shall treat the other Party's Confidential Information as confidential within their respective organizations and each Party shall be given the ability to defend the confidentiality of its Confidential Information to the maximum extent allowable under the law prior to disclosure by the other Party of such Confidential Information.
- 13.2. Subject to the requirements of the Customer's public record laws ("PRL"), neither Party shall disclose the other Party's Confidential Information to any person outside their respective organizations unless disclosure is made in response to, or because of, an obligation to any federal, state, or local governmental agency or court with appropriate jurisdiction, or to any person properly seeking discovery before any such agency or court.
- 13.3. Any specific information that Dominion claims to be confidential must be clearly marked or identified as such by the Customer. To the extent consistent with PRL, Customer shall maintain the confidentiality of all such information marked by Dominion as confidential. If a request is made to view such Confidential Information, Customer will notify Dominion of such request and the date the information will be released to the requestor unless Dominion obtains a court order enjoining such disclosure. If Dominion fails to obtain such court order enjoining such disclosure, the Customer will release the requested information on the date specified. Such release shall be deemed to have been made with Dominion's consent and shall not be deemed to be a violation of law or this Agreement.

14. Assignment. Neither Party may assign its rights, obligations, or interests in this Agreement without the written consent of the other Party, providing however that Dominion may assign the proceeds of this Agreement to a financial institution without prior consent of the Customer but with written notice to Customer.

15. Termination.

15.1 For Default. In the event either Party violates any provisions of this Agreement, the non-violating Party may serve written notice upon the violating Party identifying the violation and a providing a reasonable cure period. Except as otherwise noted herein, such cure period shall be at least thirty (30) days. In the event the violating Party has not remedied the infraction at the end of the cure period, the non-violating Party may serve written notice upon the violating Party of termination, and seek legal remedies for breach of contract as allowed hereunder. If the breach identified in the notice cannot be completely cured within the specified time period, no default shall occur if the Party receiving the notice begins curative action within the specified time period and thereafter proceeds with reasonable diligence and in good faith to cure the breach as soon as practicable.

15.2 For Non-Appropriation of Funds. The Customer shall not be obligated for payments hereunder for any future fiscal year unless or until the Customer appropriates funds for this Agreement in Customer's budget for that fiscal year. In the event that funds are not appropriated, then this Agreement may be terminated by the Customer as the end of the last fiscal year for which funds were appropriated. Termination of this Agreement by the Customer under this Section 15.2 shall not constitute a breach of this Agreement by the Customer. Customer shall notify Dominion in writing of such non-appropriation at the earliest possible date which, in any event, shall be prior to Dominion performing services during any fiscal year for which an appropriation has not been made. In the event Customer notifies Dominion that sufficient funds have not been appropriated, or if in fact sufficient funds have not been appropriated, to compensate Dominion in accordance with this Agreement, Dominion may suspend Dominion's performance and terminate all Dominion licenses under this Agreement. Suspension of performance and termination of all Dominion licenses by Dominion in accordance with this section 15.2 shall not constitute a breach of this Agreement by Dominion.

16. Legality and Severability. This Agreement and the Parties' actions under this Agreement shall comply with all applicable federal, state and local laws, ordinances, rules, regulations, court orders, and applicable governmental agency orders. If any term or provision of this Agreement is held to be illegal or unenforceable, the remainder of this Agreement shall not be affected thereby and each term or provision of this Agreement shall be valid and enforceable to the fullest extent permitted by law. The Parties agree that any court reviewing this Agreement shall reform any illegal or unenforceable provision to carry out the express intent of the parties as set forth herein to the fullest extent permitted by law.

17. Survival. The provisions of Sections 2, 9, 10, 11, 12, 13, 16, 18, and 19 shall survive the expiration or termination of this Agreement.

18. Choice of Law. Interpretation of this Agreement shall be governed by the laws of the State of California, and the courts of competent jurisdiction located in the State of California will have jurisdiction to hear and determine questions relating to this Agreement.

19. Waiver. Any failure of a Party to assert any right under this Agreement shall not constitute a waiver or a termination of that right or any provisions of this Agreement.

20. Independent Contractor. Dominion and its agents and employees are independent contractors performing professional services for the Customer and are not employees of the Customer. Dominion and its agents and employees shall not accrue leave, retirement, insurance, bonding, use of Customer vehicles, or any other benefits afforded to employees of the Customer as a result of this Agreement. Dominion acknowledges that all sums received hereunder are personally reportable by it for income tax purposes as self-employment or business income and are reportable for self-employment tax.

21. Notices. All notices required or permitted to be given hereunder shall be given in writing and shall be deemed to have been given when personally delivered or by nationally recognized overnight carrier or mailed, certified or registered mail, return receipt requested, addressed to the intended recipient as follows:

If to Dominion:

Dominion Voting Systems, Inc.
Attn: Contracts Administrator
1201 18th St., Ste. 210
Denver, CO 80202

If to the Customer:

Inyo County Clerk-Recorder
Attn: Kammi Foote, Clerk-Recorder
168 N. Edwards Street
Independence, CA 93526

22. Entire Agreement. This Agreement and its Exhibits incorporated herein by reference constitute the entire agreement, understanding and representations between Dominion and the Customer, and supersede and replace all prior agreements, written or oral. No modifications or representations to the Agreement shall be valid unless made in writing and signed by duly authorized representatives of both the Customer and Dominion, and incorporated as an Addendum hereto.

23. Third-Party Beneficiary. No person shall be a third-party beneficiary pursuant to this Agreement. No obligation of Dominion or Customer may be enforced against Dominion or Customer, as applicable, by any person not a party to this Agreement.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed as of the date first above written.

DOMINION VOTING SYSTEMS, INC.

AUTHORIZED SIGNATURE

PRINTED NAME

TITLE

DATE

INYO COUNTY, CA

AUTHORIZED SIGNATURE

PRINTED NAME

TITLE

DATE

EXHIBIT A
VOTING SYSTEM AGREEMENT
BY AND BETWEEN DOMINION VOTING SYSTEMS
AND INYO COUNTY, CA

PRICING SUMMARY AND DELIVERABLES DESCRIPTION

1. **Pricing Summary** - Prices of equipment, technical facilities, software, and other related services for voting, vote counting, and result processing. All pricing in U.S. Dollars.

Description	Quantity	Unit Price	Extended Price
ImageCast Central Tabulator Canon DR-G1130 high speed document scanner, OptiPlex 7440 All-in-One Series with pre-loaded software, ImageCast Central Software, Twain driver, ibutton driver, DR-G1130 driver, One (1) iButton Programmer and (1) iButton Key Switch & Cat5 RJ 45 Cables.	2	\$25,000	\$ 50,000
ImageCast X – BMD Accessible Units 21 inch touchscreen tablet, ICX Firmware, Tablet, ATI accessible unit, 5 voter activation cards, printer, cables, power cord	10	\$ 3,175	\$ 31,750
ImageCast X Voter Activation Stations Dell Laptop, ICX Activation software Smart Card Reader/Writer	5	\$ 1,200	\$ 6,000
ImageCast X Voting Booths	10	\$ 350	\$ 3500
ImageCast X Pollworker Smartcards	10	\$ 8	\$ 80
ImageCast X Technician Smartcards	2	\$ 8	\$ 16
Election Management Software & Hardware			
Democracy Suite Light Software	1	\$ 8,500	\$ 8,500
ImageCast Adjudication Application	1	\$ 5,000	\$ 5,000
Democracy Suite EMS Server Hardware Kit – up to 7 clients	1	\$ 12,000	\$ 12,000
Democracy Suite EMS Server Hardware Kit – Upgrade of adjudication station, client workstation and server (during the Term of the Agreement)	1	\$ 12,000	\$ 12,000
Democracy Suite EMS Workstation	1	\$ 1,400	\$ 1,400
Democracy Suite Adjudication Hardware Kit	1	\$ 1,400	\$ 1,400
EMS Report Printer	1	\$ 250	\$ 250

Shipping	<i>N/A</i>	<i>TBD</i>	<i>TBD</i>
Implementation and Training			
Project Management and Implementation Support	10	\$ 2,500	\$ 25,000
Product Implementation and Support Training	1	\$ 2,000	\$ 2,000
Democracy Suite Training	1	\$ 2,000	\$ 2,000
System Acceptance Testing Training	1	\$ 2,000	\$ 2,000
ICX Operator Training	1	\$ 2,000	\$ 2,000
ICC and Adjudication Operator Training	2	\$ 2,000	\$ 4,000
Pollworker Train the Trainer	1	\$ 2,000	\$ 2,000
Election Set Up and Support			
Election Set Up (12 Elections Total)	12	\$ 4,200	\$ 50,400
Election Day Support (2 Elections Total)	2	\$ 4,500	\$ 9,000
<i>SUBTOTAL</i>			\$ 230,296
<i>Democracy Suite Hardware Upgrade (Discount)</i>	1	<i>(\$12,000)</i>	<i>(\$12,000)</i>
<i>General Discount</i>	1	<i>(\$16,500)</i>	<i>(\$16,500)</i>
TOTAL EXTENDED PRICE			\$ 201,796

ANNUAL SOFTWARE LICENSE

(Beginning on the first anniversary of the Effective Date through the Agreement Term)

Description	Quantity	Unit Price	Extended Price
Democracy Suite Light Software	1	\$ 1,700	\$ 1,700
ImageCast Adjudication Application	1	\$ 1,000	\$ 1,000
ImageCast Central Tabulator Software	2	\$ 2,575	\$ 5,150
ImageCast X – BMD Accessible Units	10	\$ 150	\$ 1,500

* Dominion reserves the right to adjust the Annual Software License Fee within five percent (5%) of the then current fee

ANNUAL HARDWARE WARRANTY

(Beginning on the first anniversary of the Effective Date through the Agreement Term)

Description	Quantity	Unit Price	Extended Price
ImageCast Central Tabulator Software	2	\$ 1,500	\$ 3,000

ImageCast X – BMD Accessible Units	10	\$ 115	\$ 1,150
------------------------------------	----	--------	----------

2. **Payment Schedule** - Dominion shall provide invoices to the Customer as described below. The Customer shall pay invoices in a timely manner and no later than thirty (30) calendar days from receipt of a Dominion invoice. Payments specified in this Exhibit are exclusive of all excise, sale, use and other taxes imposed by any governmental authority, all of which taxes shall be reimbursed by the Customer.

ID	Payment Invoice Date	Payment Amount
1	Agreement Signing	\$121,078
2	Completion of System Acceptance	\$80,718
3	Shipping	TBD

3. **Detailed Deliverables Description**

- 3.1 **ImageCast® Central Scanner (ICC)**. Customer shall provide the ImageCast® Central Scanner for use by The Customer. The ImageCast® Central Scanner is commercial off-the-shelf digital scanners configured to work with the ImageCast® Central Software for high speed ballot tabulation. Each ImageCast® Central Scanner includes the following components:

- 3.1.1 Canon DR-G1130 high speed document scanner
- 3.1.2 ImageCast® Central Software including third party Twain software
- 3.1.3 OptiPlex 7440 All-in-One Series with pre-loaded software
- 3.1.4 iButton Security Key
- 3.1.5 iButton Programmer and iButton Key Switch & Cat5 RJ 45 Cables used with Democracy Suite to transfer security and election information to the iButtons for use with the ICC.

- 3.2 **ImageCast® Software**. The Parties will enter into software licenses for the ImageCast software, substantially in the form of Exhibit B to this Agreement. The Dominion software includes, without limitation:

- 3.2.1 **AuditMark®**. For each ballot that is scanned and accepted into the unit, a corresponding ballot image is created and stored for audit purposes. The image consists of two parts described below.

- The top portion of the image contains a scanned image of the ballot.
- The bottom portion consists of a machine-generated type-out showing each mark that the unit interpreted for that particular ballot. This is referred to as an AuditMark®.

- 3.1 **ImageCast® X ("ICX") Application** is an application used for touchscreen voting on tablets at a voting location, and a Democracy Suite election database. Voting sessions are initiated on the tablet by either a Smart card or the entry of a numeric

code based on activation. The ballot is loaded directly onto the standalone device. All voting activity is performed at the tablet, including accessible voting. Accessible voting interfaces connect to the tablet via an adapter that supports most accessible devices, allowing voters to bring their own device. After review and completion of the ballot selections, a paper ballot is created for the voter from a printer in the voting booth, and the ballot is cast after insertion in a ballot box. The ballots are scanned using ImageCast tabulator or scanner.

3.2 **Democracy Suite Light Software** consists of the following components:

3.2.1 Election File and iButton Creation Customer is authorized to create Election Files and iButtons from EED to load on the ICX, ICVA and ICC units.

3.2.2 Results, Tally and Reporting (RTR) Client Application is the application used for the tally, reporting and publishing of election results.

3.3 **ImageCast[®] Adjudication Application** is a client and server application used to review and adjudicate ImageCast[®] Central Scanner ballot images. The application uses tabulator results files and scanned images to allow election administrators to make adjudications to ballots with auditing and reporting capabilities. The Adjudication Application examines such voter exceptions as overvotes, undervotes, blank contests, blank ballots, write-in selections, and marginal marks. The application works in two basic modes: election project setup and adjudication. The Adjudication Application can be used in a multi-client environment.

3.4 **Implementation Services and Training.** Dominion will provide the following training as described herein.

3.4.1 Project Management Support. Dominion will provide project management support to oversee the general operations of the project through the Agreement Term. The project manager shall be responsible for arranging all meetings, visits and consultations between the parties and for all administrative matters such as invoices, payments and amendments. The Parties shall develop and finalize a project implementation plan including a training and delivery schedule. The Parties agree that during the course of the implementation, changes to the project schedule may be required. Any changes to the project schedule must be mutually agreed to by both Parties and such agreement shall not be unreasonably withheld.

3.4.2 ImageCast[®] X – This training introduces the ImageCast[®] X system with an emphasis on the operation of the hardware. Students can expect to learn general operations, logic and accuracy testing, Election Day setup and operation, and troubleshooting.

3.4.3 ImageCast[®] ICC – This training introduces the ImageCast[®] ICC with an emphasis on the operation of the hardware. Students can expect to learn general operations, logic and accuracy testing, ballot scanning operation, and troubleshooting.

3.4.4 EMS Server Installation, Configuration & Testing. Dominion will provide a minimum total of one (1) day of direct onsite support for EMS Server

installation, configuration & testing.

- 3.4.5 Democracy Suite[®] EMS System– This training covers the restoring election project backups, creating ICX, ICC and ICXVA files, tally and reporting.
 - 3.4.6 System Acceptance Testing Support. Dominion will provide direct onsite training and support during the System Acceptance Testing period
 - 3.4.7 Pollworker Train the Trainer – This provides training to the Customer staff on operations of a polling location including the ImageCast[®] X, ICX Card activation, testing and troubleshooting.
 - 3.4.8 On-Site Election Day Support. Dominion will provide three (3) days (inclusive of travel) of direct onsite election support for two (2) elections.
- 3.5 ***Election Ballot Definition Setup.*** Dominion shall provide election setup services and support for the election database creation and ballot review for the twelve (12) Elections during the term of the initial contract. Ballot definition services will be provided in English only and will include the following: Democracy Suite Election project setup, provide the Mail Ballot/Absentee PDF artwork, verification and proofing for each Election, provide audio setup for audio voting using a synthesizer. Any outside recording charges would be at the Customer's expense.
- 3.5.1 2018 - Primary Election
 - 3.5.2 2018 - General Election
 - 3.5.3 2020 - Primary Election
 - 3.5.4 2020 - General Election
 - 3.5.5 2022 - Primary Election
 - 3.5.6 2022 - General Election
 - 3.5.7 2024 - Primary Election
 - 3.5.8 2024 - General Election
 - 3.5.9 An additional four elections to be agreed upon by both parties
- 3.6 ***Travel and Expenses included.*** All costs of Dominion transportation, lodging and meal expenses are included during the Agreement Term.
- 3.7 ***Ongoing telephone support.*** Telephone support shall be available for Customers during the Term of the Agreement at no additional costs.
- 3.8 ***Other Services, Consumables or Equipment.*** Any other services, consumables or equipment not specifically identified in this Agreement are available for purchase by the Customer at the then current Dominion list price.
- 3.9 ***Option to Purchase additional ICX units.*** The Customer shall have an option to purchase additional ImageCast X BMD Accessible units through the 2020 calendar year at a price of \$3,175.00 per unit.

EXHIBIT B

SOFTWARE LICENSE TERMS AND CONDITIONS

1. Definitions.

- 1.1. "Agreement" shall mean the agreement between the Parties for the use of the licensed Software.
- 1.2. "Licensee" shall mean the Customer defined in the general terms and conditions of this Agreement.
- 1.3. "Licensor" shall mean Dominion Voting Systems, Inc.
- 1.4. "Party" or "Parties" Licensor and Licensee may hereinafter be referred to individually as a Party and collectively as the Parties.
- 1.5. "Software" means the Democracy Suite[®] and ImageCast[®] software licensed by Licensor hereunder, in object code form, including all documentation therefore.
- 1.6. "Specifications" means descriptions and data regarding the features, functions and performance of the Software, as set forth in user manuals or other applicable documentation provided by Licensor.
- 1.7. "Third-Party Products" means any software or hardware obtained from third-party manufacturers or distributors and provided by Licensor hereunder.

2. License Terms.

- 2.1. License to Software. Subject to the terms herein, Licensor grants Licensee a non-exclusive, non-transferrable license to use the Software solely for the Licensee's own internal business purposes and solely in conjunction with the Software and hardware. This License shall only be effective during the Term and cannot be transferred or sublicensed.
- 2.2. Print Copyright License. Subject to the Print Copyright License terms and conditions as defined in Schedule A attached hereto, Licensor grants to Licensee a non-exclusive, non-transferable print copyright license as defined in Schedule A.
- 2.3. Third-Party Products. When applicable, Licensor shall sublicense any software that constitutes or is contained in Third-Party Products, in object code form only, to Licensee for use during the Term.
- 2.4. No Other Licenses. Other than as expressly set forth herein, (a) Licensor grants no licenses, expressly or by implication, and (b) Licensor's entering into the Agreement will not be deemed to license or assign any intellectual property rights of Licensor to Licensee or any third party. Licensee agrees not to use the Software as a service bureau for elections outside the Licensee's jurisdiction and agrees not to reverse engineer or otherwise attempt to derive the source code of the Software. The Licensee shall have no power to transfer or grant sub-licenses for the Software. Any use of all or any portion of the Software not expressly permitted is strictly prohibited.

3. Payment. In consideration of the grant of the license, the Licensee shall pay the license fees set forth in Exhibit A of this Agreement.

4. Upgrades and Certification. During the Term, Licensor may provide upgrades to Licensee under the following terms and conditions.

4.1. Upgrades. In the event that Licensor, at its sole discretion, certifies a Software upgrade under the applicable laws and regulations of the State of California, Licensor shall make the certified Software upgrade available to the Licensee at no additional cost.

4.2. Certification Requirement. Notwithstanding any other terms of this Agreement, Licensor shall not provide, and shall not be obligated to provide under this Agreement any upgrade, enhancement or other software update that has not been certified under the applicable provisions of the election laws and regulations of the State of California.

5. Prohibited Acts. The Licensee shall not, without the prior written permission of Licensor:

5.1. Transfer or copy onto any other storage device or hardware or otherwise copy the Software in whole or in part except for purposes of system backup;

5.2. Reverse engineer, disassemble, decompile, decipher or analyze the Software in whole or in part;

5.3. Alter or modify the Software in any way or prepare any derivative works of the Software or any part of parts of the Software;

5.4. Alter, remove or obstruct any copyright or proprietary notices from the Software, or fail to reproduce the same on any lawful copies of the Software.

6. Return of Software. Upon termination or expiration of this Agreement, Licensee shall (i) forthwith return to Licensor all Software in its possession or control, or destroy all such Software from any electronic media, and certify in writing to Licensor that it has been destroyed.

7. Warranties. The following warranties will apply to all Software during the Term.

7.1. Software Warranty Terms. Licensor warrants that the Software will function substantially in accordance with the Specification during the Term. The Licensor also warrants that the Software shall comply with the State of California certification requirements and election laws (collectively the "Requirements") in effect as of the date the Software is certified by the State of California. This provision applies to the initially installed Software as well as any subsequent upgrades pursuant to Section 3 herein. However, the Licensor will not be required to make modifications to the Software or System as a result of changes in the Requirements. The foregoing warranty will be void in the event of the Software (i) having been modified by any party other than Licensor or (ii) having been used by the Licensee for purposes other than those for which the Software was designed by Licensor. If Licensor establishes that the reported material failure is not covered by the foregoing warranty, the Licensee shall be responsible for the costs of Licensor's investigative and remedial work at Licensor's then current rates.

7.2. Corrections. If the Licensee believes that the Software is not functioning substantially in accordance with the Specifications or Requirements, the Licensee shall provide Licensor with written notice of the material failure within thirty (30) days of discovering the material failure, provided that the Licensee can reproduce the material failure to Licensor. The Licensor shall correct the deficiencies, at no additional cost to the Licensee and incorporate such corrections into the next version certified by the State of California.

7.3 Third-Party Products. The warranties herein do not apply to any Third-Party Products. However, to the extent permitted by the manufacturers of Third-Party Products, Licensor shall pass through to Licensee all warranties such manufacturers make to Licensor regarding the operation of such Third-Party Products.

7.4. NO OTHER WARRANTIES. LICENSOR DISCLAIMS ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER WRITTEN, ORAL, EXPRESS, IMPLIED OR STATUTORY, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY BASED ON A COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE.

SCHEDULE A

PRINT COPYRIGHT LICENSE TERMS AND CONDITIONS

1. **Definitions.** For the purposes of this Agreement, the following are defined terms:
 - 1.1. "Derivative Works" shall mean any work that is based upon or derived from the Licensor's voting systems' ballots, including without limitation, sample ballots and voting booklets.
 - 1.2. "Voting Systems' Ballots" shall mean any ballot created for use with any voting system owned or licensed by the Licensor.
2. **Print Copyright License and Use.**
 - 2.1. Copyright License Grant. Licensor grants to the Licensee a non-exclusive, non-transferable copyright license to print, reproduce, distribute or otherwise copy the Licensor's Voting Systems' Ballots or any Derivative Works (collectively the "Materials") pursuant to the terms and conditions of this Schedule A.
 - 2.2. Copyright License Use. Other than as expressly set forth herein, (a) Licensor grants no other licenses, expressly or by implication, and (b) Licensor's entering into and performing the Agreement will not be deemed to license or assign any intellectual property rights of Licensor to Licensee or any third party, (c) the copyright license granted herein cannot be transferred or sublicensed and the Voting Systems' Ballots or Derivative Works cannot be reproduced by any third party without the prior written consent of the Licensor, including without limitation:
 - (i) any commercial or non-commercial printer
 - (ii) any third party vendor using ballot on demand system.
 - 2.3. Rights and Interests. All right, title and interest in the Material, including without limitation, any copyright, shall remain with the Licensor.
3. **No Copyright Warranties.** LICENSOR DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, WHETHER WRITTEN, ORAL, EXPRESS, IMPLIED OR STATUTORY, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY BASED ON A COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE.



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

For Clerk's Use Only: AGENDA NUMBER 15

- Consent Departmental Correspondence Action
 Public Hearing Scheduled Time for Closed Session Informational

FROM: HEALTH & HUMAN SERVICES – Behavioral Health Division

FOR THE BOARD MEETING OF: December 19, 2017

SUBJECT: Ratification of Mental Health Performance Contract (17-94525) with the State Department of Health Care Services for the period July 1, 2017 through June 30, 2018.

DEPARTMENTAL RECOMMENDATION:

Request Board ratify the performance contract between Inyo County Mental Health and the State of California, Department of Health Care Services (DHCS) for the provision of county mental health services for the one-year period of July 1, 2017 and June 30, 2018 and designate the HHS Deputy Director of Behavioral Health, in her role as the County Mental Health Director, to sign both copies of each contract as well as complete the Certification Clause.

CAO RECOMMENDATION:

SUMMARY DISCUSSION:

This contract comes before you for ratification as it was not received until the end of October 2017 for the current fiscal year. The contract does not have substantive changes from the prior year's contract. The Standard Performance contract sets forth the conditions that the Counties must meet to receive funds as related to the Mental Health Services Act (MHSA), Projects for Assistance in Transition from Homelessness (not accessed in Inyo), Community Mental Health Services Grant (MHSBG), and community mental health services provided with realignment funds not related to Medi-Cal services. The contract reflects the mental health programs in the Governor's mental health budget. It is the agreement by the County to comply with the statutory regulations and requirements that govern the planning, use, tracking and reporting of the mental health funds. The program specifications as related to MHSA are spelled out in detail. There are also general provisions such as maintenance of effort, program principles, reimbursement methods, quality assurance and improvement, performance outcomes, patients' rights, and record keeping as well as reference to the regulations that govern these areas. The performance contract includes exhibits that address information confidentiality and security requirements, including the HIPAA Business Associate's Agreement, and two copies of the contract certification clause. The contract also includes the signed agreement for information exchange between DHCS and the Social Security Administration.

ALTERNATIVES:



Your Board could deny approval of the performance contract. This would impact the County's ability to access the various Mental Health funds.

OTHER AGENCY INVOLVEMENT:

Mental Health and Substance Use Disorder programs are integrated as the Behavioral Health division of the HHS Department. Behavioral Health works with other HHS divisions as well as other county and community agencies such as health care, law enforcement, and schools.

FINANCING:

There is no actual dollar amount specified in this contract as it is a performance contract that outlines the conditions under which funds will be released. The funds referred to in this contract are brought in as revenue into the Mental Health budget (045200).

APPROVALS	
COUNTY COUNSEL: 	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS <i>(Must be reviewed and approved by County Counsel prior to submission to the Board Clerk.)</i> Approved: <u>YES</u> <u>12/1/17</u> Date:
AUDITOR/CONTROLLER: 	ACCOUNTING/FINANCE AND RELATED ITEMS <i>(Must be reviewed and approved by the Auditor/Controller prior to submission to the Board Clerk.)</i> Approved: <u>yes</u> <u>12/4/2017</u> Date:
PERSONNEL DIRECTOR:	PERSONNEL AND RELATED ITEMS <i>(Must be reviewed and approved by the Director of Personnel Services prior to submission to the Board Clerk.)</i> Approved: _____ Date:

DEPARTMENT HEAD SIGNATURE:

(Not to be signed until all approvals are received)

Manlyn Marmby Jody Date: 12-7-17


REGISTRATION NUMBER	AGREEMENT NUMBER 17-94525
---------------------	------------------------------

- This Agreement is entered into between the State Agency and the Contractor named below:

STATE AGENCY'S NAME Department of Health Care Services	(Also known as DHCS, CDHS, DHS or the State)
CONTRACTOR'S NAME Inyo County Mental Health	(Also referred to as Contractor)
- The term of this Agreement is: July 1, 2017 through June 30, 2018
- The maximum amount of this Agreement is: \$ 0
Zero dollars
- The parties agree to comply with the terms and conditions of the following exhibits, which are by this reference made a part of this Agreement.

Exhibit A – Program Specifications (including Special Terms and Conditions)	16 pages
Exhibit A – Attachment I – Request for Waiver	1 page
Exhibit B – Funds Provision	1 page
Exhibit C * – General Terms and Conditions	<u>GTC 04/2017</u>
Exhibit D – Information Confidentiality and Security Requirements	7 pages
Exhibit E – Privacy and Information Security Provisions (including Attachment A)	31 pages
Exhibit E – Attachment B – Information Security Exchange Agreement between the Social Security Administration (SSA) and the California Department of Health Care Services (DHCS)	101 pages

Items shown above with an Asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto. These documents can be viewed at <http://www.dgs.ca.gov/ols/Resources/StandardContractLanguage.aspx>.

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

CONTRACTOR		California Department of General Services Use Only
CONTRACTOR'S NAME (if other than an individual, state whether a corporation, partnership, etc.) Inyo County Mental Health		
BY (Authorized Signature) 	DATE SIGNED (Do not type)	
PRINTED NAME AND TITLE OF PERSON SIGNING Gail Zwier, PhD, Director		
ADDRESS 162 J Grove Street Bishop, CA 93514		
STATE OF CALIFORNIA		
AGENCY NAME Department of Health Care Services		
BY (Authorized Signature) 	DATE SIGNED (Do not type)	
PRINTED NAME AND TITLE OF PERSON SIGNING Don Rodriguez, Chief, Contract Management Unit		
ADDRESS 1501 Capitol Avenue, Suite 71.5195, MS 1403, P.O. Box 997413, Sacramento, CA 95899-7413		
		<input checked="" type="checkbox"/> Exempt per: W&I Code §14703

REGISTRATION NUMBER	AGREEMENT NUMBER 17-94525
---------------------	------------------------------

- This Agreement is entered into between the State Agency and the Contractor named below:
 STATE AGENCY'S NAME (Also known as DHCS, CDHS, DHS or the State)
 Department of Health Care Services
 CONTRACTOR'S NAME (Also referred to as Contractor)
 Inyo County Mental Health
- The term of this Agreement is: July 1, 2017 through June 30, 2018
- The maximum amount of this Agreement is: \$ 0
Zero dollars
- The parties agree to comply with the terms and conditions of the following exhibits, which are by this reference made a part of this Agreement.

Exhibit A – Program Specifications (including Special Terms and Conditions)	16 pages
Exhibit A – Attachment I – Request for Waiver	1 page
Exhibit B – Funds Provision	1 page
Exhibit C * – General Terms and Conditions	<u>GTC 04/2017</u>
Exhibit D – Information Confidentiality and Security Requirements	7 pages
Exhibit E – Privacy and Information Security Provisions (including Attachment A)	31 pages
Exhibit E – Attachment B – Information Security Exchange Agreement between the Social Security Administration (SSA) and the California Department of Health Care Services (DHCS)	101 pages

Items shown above with an Asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto. These documents can be viewed at <http://www.dgs.ca.gov/ols/Resources/StandardContractLanguage.aspx>.

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

CONTRACTOR		California Department of General Services Use Only
CONTRACTOR'S NAME (if other than an individual, state whether a corporation, partnership, etc.) Inyo County Mental Health		
BY (Authorized Signature) 	DATE SIGNED (Do not type)	
PRINTED NAME AND TITLE OF PERSON SIGNING Gail Zwier, PhD, Director		
ADDRESS 162 J Grove Street Bishop, CA 93514		
STATE OF CALIFORNIA		
AGENCY NAME Department of Health Care Services		<input checked="" type="checkbox"/> Exempt per: W&I Code §14703
BY (Authorized Signature) 	DATE SIGNED (Do not type)	
PRINTED NAME AND TITLE OF PERSON SIGNING Don Rodriguez, Chief, Contract Management Unit		
ADDRESS 1501 Capitol Avenue, Suite 71.5195, MS 1403, P.O. Box 997413, Sacramento, CA 95899-7413		

CCC 04/2017

CERTIFICATION

I, the official named below, CERTIFY UNDER PENALTY OF PERJURY that I am duly authorized to legally bind the prospective Contractor to the clause(s) listed below. This certification is made under the laws of the State of California.

<i>Contractor/Bidder Firm Name (Printed)</i> Inyo County Mental Health		<i>Federal ID Number</i>
<i>By (Authorized Signature)</i>		
<i>Printed Name and Title of Person Signing</i>		
<i>Date Executed</i>	<i>Executed in the County of</i>	

CONTRACTOR CERTIFICATION CLAUSES

1. STATEMENT OF COMPLIANCE: Contractor has, unless exempted, complied with the nondiscrimination program requirements. (Gov. Code §12990 (a-f) and CCR, Title 2, Section 11102) (Not applicable to public entities.)

2. DRUG-FREE WORKPLACE REQUIREMENTS: Contractor will comply with the requirements of the Drug-Free Workplace Act of 1990 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.

b. Establish a Drug-Free Awareness Program to inform employees about:

- 1) the dangers of drug abuse in the workplace;
- 2) the person's or organization's policy of maintaining a drug-free workplace;
- 3) any available counseling, rehabilitation and employee assistance programs; and,
- 4) penalties that may be imposed upon employees for drug abuse violations.

c. Every employee who works on the proposed Agreement will:

- 1) receive a copy of the company's drug-free workplace policy statement; and,
- 2) agree to abide by the terms of the company's statement as a condition of employment on the Agreement.

Failure to comply with these requirements may result in suspension of payments under the Agreement or termination of the Agreement or both and Contractor may be ineligible for award of any future State agreements if the department determines that any of the following has occurred: the Contractor has made false certification, or violated the

certification by failing to carry out the requirements as noted above. (Gov. Code §8350 et seq.)

3. NATIONAL LABOR RELATIONS BOARD CERTIFICATION: Contractor certifies that no more than one (1) final unappealable finding of contempt of court by a Federal court has been issued against Contractor within the immediately preceding two-year period because of Contractor's failure to comply with an order of a Federal court, which orders Contractor to comply with an order of the National Labor Relations Board. (Pub. Contract Code §10296) (Not applicable to public entities.)

4. CONTRACTS FOR LEGAL SERVICES \$50,000 OR MORE- PRO BONO REQUIREMENT: Contractor hereby certifies that Contractor will comply with the requirements of Section 6072 of the Business and Professions Code, effective January 1, 2003.

Contractor agrees to make a good faith effort to provide a minimum number of hours of pro bono legal services during each year of the contract equal to the lesser of 30 multiplied by the number of full time attorneys in the firm's offices in the State, with the number of hours prorated on an actual day basis for any contract period of less than a full year or 10% of its contract with the State.

Failure to make a good faith effort may be cause for non-renewal of a state contract for legal services, and may be taken into account when determining the award of future contracts with the State for legal services.

5. EXPATRIATE CORPORATIONS: Contractor hereby declares that it is not an expatriate corporation or subsidiary of an expatriate corporation within the meaning of Public Contract Code Section 10286 and 10286.1, and is eligible to contract with the State of California.

6. SWEATFREE CODE OF CONDUCT:

a. All Contractors contracting for the procurement or laundering of apparel, garments or corresponding accessories, or the procurement of equipment, materials, or supplies, other than procurement related to a public works contract, declare under penalty of perjury that no apparel, garments or corresponding accessories, equipment, materials, or supplies furnished to the state pursuant to the contract have been laundered or 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 the contractor's records, documents, agents or employees, or premises if reasonably required by authorized officials of the contracting agency, the Department of Industrial Relations,

or the Department of Justice to determine the contractor's compliance with the requirements under paragraph (a).

7. DOMESTIC PARTNERS: For contracts of \$100,000 or more, Contractor certifies that Contractor is in compliance with Public Contract Code section 10295.3.

8. GENDER IDENTITY: For contracts of \$100,000 or more, Contractor certifies that Contractor is in compliance with Public Contract Code section 10295.35.

DOING BUSINESS WITH THE STATE OF CALIFORNIA

The following laws apply to persons or entities doing business with the State of California.

1. CONFLICT OF INTEREST: Contractor needs to be aware of the following provisions regarding current or former state employees. If Contractor has any questions on the status of any person rendering services or involved with the Agreement, the awarding agency must be contacted immediately for clarification.

Current State Employees (Pub. Contract Code §10410):

1). No officer or employee shall engage in any employment, activity or enterprise from which the officer or employee receives compensation or has a financial interest and which is sponsored or funded by any state agency, unless the employment, activity or enterprise is required as a condition of regular state employment.

2). No officer or employee shall contract on his or her own behalf as an independent contractor with any state agency to provide goods or services.

Former State Employees (Pub. Contract Code §10411):

1). For the two-year period from the date he or she left state employment, no former state officer or employee may enter into a contract in which he or she engaged in any of the negotiations, transactions, planning, arrangements or any part of the decision-making process relevant to the contract while employed in any capacity by any state agency.

2). For the twelve-month period from the date he or she left state employment, no former state officer or employee may enter into a contract with any state agency if he or she was employed by that state agency in a policy-making position in the same general subject area as the proposed contract within the 12-month period prior to his or her leaving state service.

If Contractor violates any provisions of above paragraphs, such action by Contractor shall render this Agreement void. (Pub. Contract Code §10420)

Members of boards and commissions are exempt from this section if they do not receive payment other than payment of each meeting of the board or commission, payment for preparatory time and payment for per diem. (Pub. Contract Code §10430 (e))

2. LABOR CODE/WORKERS' COMPENSATION: Contractor needs to be aware of the provisions which require every employer to be insured against liability for Worker's Compensation or to undertake self-insurance in accordance with the provisions, and Contractor affirms to comply with such provisions before commencing the performance of the work of this Agreement. (Labor Code Section 3700)

3. AMERICANS WITH DISABILITIES ACT: Contractor assures the State that it complies with the Americans with Disabilities Act (ADA) of 1990, which prohibits discrimination on the basis of disability, as well as all applicable regulations and guidelines issued pursuant to the ADA. (42 U.S.C. 12101 et seq.)

4. CONTRACTOR NAME CHANGE: An amendment is required to change the Contractor's name as listed on this Agreement. Upon receipt of legal documentation of the name change the State will process the amendment. Payment of invoices presented with a new name cannot be paid prior to approval of said amendment.

5. CORPORATE QUALIFICATIONS TO DO BUSINESS IN CALIFORNIA:

a. When agreements are to be performed in the state by corporations, the contracting agencies will be verifying that the contractor is currently qualified to do business in California in order to ensure that all obligations due to the state are fulfilled.

b. "Doing business" is defined in R&TC Section 23101 as actively engaging in any transaction for the purpose of financial or pecuniary gain or profit. Although there are some statutory exceptions to taxation, rarely will a corporate contractor performing within the state not be subject to the franchise tax.

c. Both domestic and foreign corporations (those incorporated outside of California) must be in good standing in order to be qualified to do business in California. Agencies will determine whether a corporation is in good standing by calling the Office of the Secretary of State.

6. RESOLUTION: A county, city, district, or other local public body must provide the State with a copy of a resolution, order, motion, or ordinance of the local governing body which by law has authority to enter into an agreement, authorizing execution of the agreement.

7. AIR OR WATER POLLUTION VIOLATION: Under the State laws, the Contractor shall not be: (1) in violation of any order or resolution not subject to review promulgated by the State Air Resources Board or an air pollution control district; (2) subject to cease and desist order not subject to review issued pursuant to Section 13301 of the Water Code for violation of waste discharge requirements or discharge prohibitions; or (3) finally determined to be in violation of provisions of federal law relating to air or water pollution.

8. PAYEE DATA RECORD FORM STD. 204: This form must be completed by all contractors that are not another state agency or other governmental entity.

Exhibit A
Program Specifications

1. Service Overview

The California Department of Health Care Services (hereafter referred to as DHCS or Department) administers the Mental Health Services Act, Projects for Assistance in Transition from Homelessness (PATH) and Community Mental Health Services Grant (MHBG) programs and oversees county provision of community mental health services provided with realignment funds. Contractor (hereafter referred to as County in this Exhibit) must meet certain conditions and requirements to receive funding for these programs and community mental health services. This Agreement, which is County's performance contract, as required by Welfare and Institutions Code (Welf. & Inst. Code) sections 5650(a), 5651, 5666, 5897, and Title 9, California Code of Regulations (Cal. Code Regs.), Title 9, section 3310, sets forth conditions and requirements that County must meet in order to receive this funding. This Agreement does not cover federal financial participation or State general funds as they relate to Medi-Cal services provided through the Mental Health Plan Contracts. County agrees to comply with all of the conditions and requirements described herein.

DHCS shall monitor this Agreement to ensure compliance with applicable federal and State law and applicable regulations. (Gov. Code §§ 11180-11182; Welf. & Inst. Code §§ 5614, 5651, subd. (c), subd. (b) &, 14124.2, subd. (a).)

2. Service Location

The services shall be performed at appropriate sites as described in this contract.

3. Service Hours

The services shall be provided during times required by this contract.

4. Project Representatives

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

Department of Health Care Services Contract Manager: Erika Cristo Telephone: (916) 552-9055 Fax: (916) 440-7620 Email: Erika.Cristo@dhcs.ca.gov	Inyo County Mental Health Contract Manager: Gail Zwier, PhD Telephone: (760) 873-6533 Fax: (760) 873-3277 Email: gzwier@inyocounty.us
--	--

B. Direct all inquiries to:

Exhibit A
Program Specifications

Department of Health Care Services	Inyo County Mental Health
Mental Health Services Division/Program Policy Unit Attention: Guy Stewart 1500 Capitol Avenue, MS 2702 P.O. Box Number 997413 Sacramento, CA, 95899-7413	Attention: Gail Zwier, PhD 162 J Grove Street Bishop, CA 93514
Telephone: (916) 449-5997 Fax: (916) 440-7620 Email: Guy.Stewart@dhcs.ca.gov	Telephone: (760) 873-6533 Fax: (760) 873-3277 Email: gzwier@inyocounty.us

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

5. General Requirements for Agreement

Welfare and Institutions Code section 5651 provides specific assurances, which are listed below, that must be included in this Agreement. County shall:

- A. Comply with the expenditure requirements of Welfare and Institutions Code Section 17608.05,
- B. Provide services to persons receiving involuntary treatment as required by Part 1 (commencing with section 5000) and Part 1.5 (commencing with section 5585) of Division 5 of the Welfare and Institution Code,
- C. Comply with all of the requirements necessary for Medi-Cal reimbursement for mental health treatment services and case management programs provided to Medi-Cal eligible individuals, including, but not limited to, the provisions set forth in Chapter 3 (commencing with section 5700) of the Welfare and Institutions Code, and submit cost reports and other data to DHCS in the form and manner determined by the DHCS,
- D. Ensure that the Local Mental Health Advisory Board has reviewed and approved procedures ensuring citizen and professional involvement at all stages of the planning process pursuant to Welfare and Institutions Code section 5604.2,
- E. Comply with all provisions and requirements in law pertaining to patient rights,
- F. Comply with all requirements in federal law and regulation pertaining to federally funded mental health programs,
- G. Provide all data and information set forth in Sections 5610 and 5664 of the Welfare and Institutions Code,

Exhibit A
Program Specifications

- H. If the County elects to provide the services described in Chapter 2.5 (commencing with Section 5670) of Division 5 of the Welfare and Institution Code, comply with guidelines established for program initiatives outlined in this chapter, and
- I. Comply with all applicable laws and regulations for all services delivered, including all laws, regulations, and guidelines of the Mental Health Services Act.

6. Services Authority

County shall adhere to the program principles and, to the extent funds are available, County shall provide the array of treatment options in accordance with Welfare and Institutions Code sections 5600.4 through 5600.7, inclusive.

A. THE MENTAL HEALTH SERVICES ACT PROGRAM

1) Program Description

Proposition 63, which created the Mental Health Services Act (MHSA), was approved by the voters of California on November 2, 2004. The Mental Health Services (MHS) Fund, which provides funds to counties for the implementation of its MHSA programs, was established pursuant to Welfare and Institutions Code section 5890. The MHSA was designed to expand California's public mental health programs and services through funding received by a one percent tax on personal incomes in excess of \$1 million. Counties use this funding for projects and programs for prevention and early intervention, community services and supports, workforce development and training, innovation, plus capital facilities and technological needs through mental health projects and programs. The State Controller distributes MHS Funds to the counties to plan for and provide mental health programs and other related activities outlined in a county's three-year program and expenditure plan or annual update. MHS Funds are distributed by the State Controller's Office to the counties on a monthly basis.

DHCS shall monitor County's use of MHS Funds to ensure that the county meets the MHSA and MHS Fund requirements. (Gov. Code §§ 11180-11182; Welf. & Inst. Code §§ 5651(c), 5897(d), 14124.2(a).)

2) Issue Resolution Process

County shall have an Issue Resolution Process (Process) to handle client disputes related to the provision of their mental health services. The Process shall be completed in an expedient and appropriate manner. County shall develop a log to record issues submitted as part of the Process. The log shall contain the date the issue was received; a brief synopsis of the issue; the final issue resolution outcome; and the date the final issue resolution was reached.

3) Revenue and Expenditure Report

Exhibit A
Program Specifications

County shall submit its Revenue and Expenditure Report (RER) electronically to the Department and the Mental Health Services Oversight and Accountability Commission by December 31 following the close of the fiscal year in accordance with Welfare and Institutions Code sections 5705 and 5899, regulations and DHCS-issued guidelines. The RER shall be certified by the mental health director and the County's auditor-controller (or equivalent), using the DHCS-issued certification form. Data submitted shall be full and complete.

If County does not submit the RER by the required deadline, DHCS may withhold MHSA funds until the reports are submitted or require the county to submit a corrective action plan with specific timelines. (Welf. & Inst. Code § § 5897(e) and 5899(e); Cal. Code Regs., tit. 9, § 3510(c)) If the RER does not meet the requirements outlined above, DHCS may request a plan of correction with specific timelines. (Welf. & Inst. Code § 5897(e)) If the RER does not meet the requirements, in accordance with the procedure in paragraph 9, DHCS may withhold payments from the MHS Fund until the County submits a complete RER. (Welf. & Inst. Code §§ 5655, Cal. Code Regs., tit. 9 § 3510(c).)

4) Distribution and Use of Local Mental Health Services Funds:

- a. Welfare and Institutions Code section 5891(c) provides that commencing July 1, 2012, on or before the 15th day of each month, pursuant to a methodology provided by DHCS, the State Controller shall distribute to County's Local Mental Health Services Fund (MHS Fund) (established by County pursuant to Welfare & Institutions Code section 5892, subd. (f)) all unexpended and unreserved funds on deposit as of the last day of the prior month in the Mental Health Services Fund for the provision of specified programs and other related activities.
- b. County shall allocate the monthly Local MHS Fund in accordance with Welfare and Institutions Code section 5892 as follows:
 - i. Twenty percent of the funds shall be used for prevention and early intervention (PEI) programs in accordance with Welfare and Institutions Code section 5840. The expenditure for PEI may be increased by County if DHCS determines that the increase will decrease the need and cost for additional services to severely mentally ill persons in County by an amount at least commensurate with the proposed increase.
 - ii. The balance of funds shall be distributed to County's mental health programs for services to persons with severe mental illnesses pursuant to Part 4 of Division 5 of the Welfare and Institutions Code, (commencing with Section 5850), for the children's system of care and Part 3 of Division 5 of the Welfare and Institutions Code (commencing with Section 5800), for the adult and older adult system of care.
 - iii. Five percent of the total funding for the County's mental health programs established pursuant to Part 3 of Division 5 of the Welfare and Institutions Code (commencing with Section 5800), Part 3.6 of Division 5 of the Welfare

Exhibit A
Program Specifications

and Institutions Code (commencing with Section 5840), and Part 4 of Division 5 of the Welfare and Institutions Code (commencing with Section 5850) shall be utilized for innovative programs in accordance with Welfare and Institutions Code sections 5830, 5847 and 5848.

- iv. Programs for services pursuant to Part 3 of Division 5 of the Welfare and Institutions Code (commencing with Section 5850) may include funds for technological needs and capital facilities, human resource needs, and a prudent reserve to ensure services do not have to be significantly reduced in years in which revenues are below the average of previous years. The total allocation for these purposes shall not exceed 20 percent of the average amount of funds allocated to County for the previous five years.
 - v. Allocations in Subparagraphs i. through iii. above, include funding for annual planning costs pursuant to Welfare and Institutions Code section 5848. The total of these costs shall not exceed five percent of the total annual revenues received for the Local MHS Fund. The planning costs shall include moneys for County's mental health programs to pay for the costs of having consumers, family members, and other stakeholders participate in the planning process and for the planning and implementation required for private provider contracts to be significantly expanded to provide additional services.
 - c. County shall use Local MHS Fund monies to pay for those portions of the mental health programs/services for children and adults for which there is no other source of funds available. (Welf. & Inst. Code §§ 5813.5, subd. (b), 5878.3 subd. (a); Cal. Code Regs., tit. 9 § 3610, subd. (d).)
 - d. County shall only use Local MHS Funds to expand mental health services. These funds shall not be used to supplant existing state or county funds utilized to provide mental health services. These funds shall only be used to pay for the programs authorized in Welfare and Institutions Code section 5892. These funds may not be used to pay for any other program and may not be loaned to County's general fund or any other County fund for any purpose. (Welf. & Inst. Code § 5891, subd. (a).)
 - e. All expenditures for County mental health programs shall be consistent with a currently approved three-year program and expenditure plan or annual update pursuant to Welfare and Institutions Code section 5847. (Welf. & Inst. Code § 5892, subd. (g).)
- 5) Three-Year Program and Expenditure Plan and Annual Updates:
- a. County shall prepare and submit a three-year program and expenditure plan, and annual updates, adopted by County's Board of Supervisors, to the Mental Health Services Oversight and Accountability Commission (MHSOAC) and DHCS within 30 calendar days after adoption. (Welf. & Inst. Code, § 5847 subd. (a).) The three-year program and expenditure plan and annual updates shall include all of the following:

Exhibit A
Program Specifications

- i. A program for Prevention and Early Intervention (PEI) in accordance with Part 3.6 of Division 5 of the Welfare and Institutions Code (commencing with Section 5840). (Welf. & Inst. Code, § 5847, subd. (b)(1).)
- ii. A program for services to children in accordance with Part 4 of Division 5 of the Welfare and Institutions Code (commencing with Section 5850), to include a wraparound program pursuant to Chapter 4 of Part 6 of Division 9 of the Welfare and Institutions Code (commencing with Section 18250), or provide substantial evidence that it is not feasible to establish a wraparound program in the County. (Welf. & Inst. Code § 5847, subd. (b)(2).)
- iii. A program for services to adults and seniors in accordance with Part 3 of Division 5 of the Welfare and Institutions Code (commencing with Section 5800). (Welf. & Inst. Code § 5847, subd. (b)(3).)
- iv. A program for innovations in accordance with Part 3.2 of Division 5 of the Welfare and Institutions Code (commencing with Section 5830). (Welf. & Inst. Code § 5847, subd. (b)(4).) Counties shall expend funds for their innovation programs upon approval by the Mental Health Services Oversight and Accountability Commission. (Welf. & Inst. Code, § 5830, subd. (e).)
- v. A program for technological needs and capital facilities needed to provide services pursuant to Part 3 of Division 5 of the Welfare and Institutions Code (commencing with Section 5800), Part 3.6 of Division 5 of the Welfare and Institutions Code (commencing with Section 5840), and Part 4 of Division 5 of the Welfare and Institutions Code (commencing with Section 5850). All plans for proposed facilities with restrictive settings shall demonstrate that the needs of the people to be served cannot be met in a less restrictive or more integrated setting. (Welf. & Inst. Code, § 5847, subd. (b)(5).)
- vi. Identification of shortages in personnel to provide services pursuant to the above programs and the additional assistance needed from the education and training programs established pursuant to Part 3.1 of Division 5 of the Welfare and Institutions Code (commencing with Section 5820) and California Code of Regulations, Title 9, section 3830, subdivision(b). (Welf. & Inst. Code § 5847, subd. (b)(6).)
- vii. Establishment and maintenance of a prudent reserve to ensure the County program will continue to be able to serve children, adults, and seniors that it is currently serving pursuant to Part 3 of Division 5 of the Welfare and Institutions Code (commencing with Section 5800), Part 3.6 of Division 5 of the Welfare and Institutions Code (commencing with Section 5840), and Part 4 of Division 5 of the Welfare and Institutions Code (commencing with Section 5850), during years in which revenues for the MHS Fund are below recent averages adjusted by changes in the state population and the California Consumer Price Index. (Welf. & Inst. Code, § 5847, subd. (b)(7).)

Exhibit A
Program Specifications

- viii. Certification by County's mental health director, which ensures that County has complied with all pertinent regulations, laws, and statutes of the MHSA, including stakeholder participation and non-supplantation requirements. (Welf. & Inst. Code, § 5847, subd. (b)(8).)
 - ix. Certification by County's Mental Health Director and County's Auditor-Controller that the County has complied with any fiscal accountability requirements as directed by DHCS, and that all expenditures are consistent with the requirements of the MHSA pursuant to California Code of Regulations, Title 9, sections 3500 and 3505. (Welf. & Inst. Code, § 5847, subd. (b)(9).)
 - b. County shall include services in the programs described in Subparagraphs 5.a.i. through 5.a.v., inclusive, to address the needs of transition age youth between the ages of 16 and 25 years old, including the needs of transition age foster youth. (Welf. & Inst. Code, § 5847, subd. (c).)
 - c. County shall prepare expenditure plans for the programs described in Subparagraphs 5.a.i. through 5.a.v., inclusive, and annual expenditure updates. Each expenditure plan update shall indicate the number of children, adults, and seniors to be served, and the cost per person. The expenditure update shall include utilization of unspent funds allocated in the previous year and the proposed expenditure for the same purpose. (Welf. & Inst. Code, § 5847, subd. (e).)
 - d. County's three-year program and expenditure plan and annual updates shall include reports on the achievement of performance outcomes for services provided pursuant to the Adult and Older Adult Mental Health System of Care Act, Prevention and Early Intervention, and the Children's Mental Health Services Act, which are funded by the MHS Fund and established jointly by DHCS and the MHSOAC, in collaboration with the California Mental Health Director's Association (Welf. & Inst. Code, § 5848, subd. (c).) County contracts with providers shall include the performance goals from the County's three-year program and expenditure plan and annual updates that apply to each provider's programs and services
 - e. County's three-year program and expenditure plan and annual update shall consider ways to provide services to adults and older adults that are similar to those established pursuant to the Mentally Ill Offender Crime Reduction Grant Program. Funds shall not be used to pay for persons incarcerated in state prison or parolees from state prisons. (Welf. & Inst. Code, § 5813.5, subd. (f).)
- 6) Planning Requirements and Stakeholder Involvement:
- a. County shall develop its three-year program and expenditure plan and annual update with local stakeholders, including adults and seniors with severe mental

Exhibit A
Program Specifications

illness, families of children, adults, and seniors with severe mental illness, providers of services, law enforcement agencies, education, social services agencies, veterans, representatives from veterans organizations, providers of alcohol and drug services, health care organizations, and other important interests. Counties shall demonstrate a partnership with constituents and stakeholders throughout the process that includes meaningful stakeholder involvement on mental health policy, program planning, and implementation, monitoring, quality improvement, evaluation, and budget allocations. County shall prepare and circulate a draft plan and update for review and comment for at least 30 calendar days to representatives of stakeholder interests and any interested party who has requested a copy of the draft plans. (Welf. & Inst. Code, § 5848, subd. (a); Cal. Code Regs., tit. 9, §§ 3300, 3310, 3315 & 3320.)

- b. County's mental health board, established pursuant to Welfare and Institutions Code, section 5604, shall conduct a public hearing on the County's draft three-year program and expenditure plan and annual updates at the close of the 30 calendar day comment period. Each adopted three-year program and expenditure plan or annual update shall summarize and analyze substantive recommendations and describe substantive changes to the three-year program and expenditure plan and annual updates. The County's mental health board shall review the adopted three-year program and expenditure plan and annual updates and recommend revisions to the County's mental health department. (Welf. & Inst. Code, § 5848, subd. (b); Cal. Code Regs., tit. 9, § 3315.)
- c. The County shall provide for a Community Planning Process as the basis for developing the Three-Year Program and Expenditure Plans and updates. The County shall designate positions and or units responsible for: the overall Community Program Planning Process; coordination and management of the Community Program Planning Process; ensuring stakeholders have the opportunity to participate; ensuring that stakeholders reflect the diversity of the demographics of the County; providing outreach to clients and their family members. The Community Program Planning process shall, at a minimum, include: involvement of clients and their family members in all aspects of the Process; participation of stakeholders; training, as needed, to County staff and stakeholders, clients, and family members regarding the stakeholder process. (Cal. Code Regs., tit. 9, § 3300.)
- d. The County shall adopt the following standards in planning, implementing, and evaluating the programs and/or services provided with MHSA funds; community collaboration, as defined in California Code of Regulations, Title 9, section 3200.060; cultural competence, as defined in section 3200.100; client driven, as defined in section 3200.050; family driven, as defined in section 3200.120; wellness, recovery and resilience focused; and integrated service experiences for clients and their families, as defined in section 3200.190. The planning, implementation and evaluation process includes, but is not limited to, the Community Program Planning Process; development of the Three-Year Program and Expenditure Plans and updates; and the manner in which the County

Exhibit A
Program Specifications

delivers services and evaluates service delivery. (Cal. Code Regs., tit. 9, § 3320)

7) County Requirements for Handling MHSA Funds

- a. County shall place all funds received from the State MHS Fund into a Local MHS Fund. The Local MHS Fund balance shall be invested consistent with other County funds and the interest earned on the investments shall be transferred into the Local MHS Fund. (Welf. & Inst. Code, § 5892, subd. (f).)
- b. The earnings on investment of these funds shall be available for distribution from the fund in future years. (Welf. & Inst. Code, § 5892, subd. (f).)
- c. Other than funds placed in a reserve in accordance with an approved plan, any funds allocated to County which it has not spent for the authorized purpose within the three years shall revert to the State. County may retain MSHA Funds for capital facilities, technological needs, or education and training for up to 10 years before reverting to the State. (Welf. & Inst. Code, § 5892, subd. (h).)
- d. When accounting for all receipts and expenditures of MHSA funds, County must adhere to uniform accounting standards and procedures that conform to the Generally Accepted Accounting Principles (GAAP), as prescribed by the State Controller in California Code of Regulations, Title 2, division 2, chapter 2, subchapter 1, Accounting Procedures for Counties, sections 901-949, and a manual, which is currently entitled "Accounting Standards and Procedures for Counties" and available at http://www.sco.ca.gov/pubs_guides.html. (Gov. Code, §30200.)

8) Department Compliance Investigations:

DHCS may investigate County's performance of the Mental Health Services Act related provisions of this Agreement and compliance with the provisions of the Mental Health Services Act, and relevant regulations. In conducting such an investigation DHCS may inspect and copy books, records, papers, accounts, documents and any writing as defined by Evidence Code Section 250 that is pertinent or material to the investigation of the County. For purposes of this Paragraph "provider" means any person or entity that provides services, goods, supplies or merchandise, which are directly or indirectly funded pursuant to MHSA. (Gov. Code §§ 11180, 11181, 11182; Welf. & Inst. Code §§ 5651, subd. (a)(9), 5897(d) 14124.2.)

9) County Breach, Plan of Correction and Withholding of State Mental Health Funds:

- a. If DHCS determines that County is out-of-compliance with the Mental Health Services Act related provisions of this Agreement, DHCS may request that County submit a plan of correction, including a specific timeline to correct the deficiencies, to DHCS. (Welf. & Inst. Code § 5897(d).)

Exhibit A
Program Specifications

- b. In accordance with Welfare and Institutions Code section 5655, if DHCS considers County to be substantially out-of-compliance with any provision of the Mental Health Services Act or relevant regulations, including all reporting requirements, the director shall order County to appear at a hearing before the Director or the Director's designee to show cause why the Department should not take administrative action. County shall be given at least twenty (20) days notice before the hearing.
- c. If the Director determines that there is or has been a failure, in a substantial manner, on the part of County to comply with any provision of the Welfare and Institutions Code or its implementing regulations, and that administrative sanctions are necessary, the Department may invoke any, or any combination of, the following sanctions Welfare and Institutions Code Section 5655:
 - 1) Withhold part or all state mental health funds from County.
 - 2) Require County to enter into negotiations with DHCS to agree on a plan for County to address County's non-compliance.
 - 3) Bring an action in mandamus or any other action in court as may be appropriate to compel compliance. Any action filed in accordance with the section shall be entitled to a preference in setting a date for hearing.

B. PROJECTS FOR ASSISTANCE IN TRANSITION FROM HOMELESSNESS (PATH) PROGRAM (42, U.S.C. §§, 290cc-21 -290cc-35, inclusive)

Pursuant to Title 42 of the United States Code, sections 290cc-21 through 290cc-35, inclusive, the State of California has been awarded federal homeless funds through the federal McKinney Projects for Assistance in Transition from Homelessness (PATH) formula grant. The PATH grant funds community based outreach, mental health and substance abuse referral/treatment, case management and other support services, as well as a limited set of housing services for the homeless mentally ill.

County shall submit its Request for Application (RFA) responses and required documentation specified in DHCS' RFA to receive PATH funds. County shall complete its RFA responses in accordance with the instructions, enclosures and attachments available on the DHCS website at:

<http://www.dhcs.ca.gov/services/MH/Pages/PATH.aspx>.

If County applied for and DHCS approved its request to receive PATH grant funds, the RFA, County's RFA responses and required documentation, and DHCS' approval constitute provisions of this Agreement and are incorporated by reference herein. County shall comply with all provisions of the RFA and the County's RFA responses.

Exhibit A
Program Specifications

C. COMMUNITY MENTAL HEALTH SERVICES GRANT (MHBG) PROGRAM (42, U.S.C. § 300x-1 et seq.)

Pursuant to Title 42, United States Code section 300x-1 et seq., the State of California has been awarded the federal Community Mental Health Services Block Grant funds (known as Mental Health Block Grant (MHBG)). County mental health agencies utilize MHBG funding to provide a broad array of mental health services within their mental health system of care (SOC) programs. These programs provide services to the following target populations: children and youth with serious emotional disturbances (SED) and adults and older adults with serious mental illnesses (SMI).

County shall submit its RFA responses and required documentation specified in DHCS' RFA to receive MHBG funding. County shall complete its RFA responses in accordance with the instructions, enclosures and attachments available on the DHCS website at:

<http://www.dhcs.ca.gov/services/MH/Pages/MHBG.aspx>.

If County applied for and DHCS approved its request to receive MHBG grant funds, the RFA, County's RFA responses and required documentation, and DHCS' approval constitute provisions of this Agreement and are incorporated by reference herein. County shall comply with all provisions of the RFA and the County's RFA responses.

7. Data Information and Submission Requirements

County shall comply with all data and information submission requirements specified in this Agreement

- A. County shall provide all applicable data and information required by federal and/or State law in order to receive any funds to pay for its MHSA programs, PATH grant (if the County receives funds from this grant), MHBG grant (if the County receives funds from this grant), or county provision of community mental health services provided with 1991 realignment funds (other than Medi-Cal). These federal and State laws include, Title 42 of the United States Code, sections 290cc-21 through 290cc-35 and 300x through 300x-9, inclusive, Welfare & Institutions Code sections 5610 and 5664 and the regulations that implement, interpret or make specific, these federal and State laws and any DHCS-issued guidelines that relate to the programs or services.
- B. County shall comply with DHCS reporting requirements related to the County's receipt of federal or State funding for mental health programs. County shall submit complete and accurate information to DHCS, and as applicable the Mental Health Services Oversight and Accountability Commission, including, but not limited, to the following:
 - 1) Client and Service Information (CSI) System Data, as specified in Title 9 of the California Code of Regulations, section 3530.10 (See subparagraph c of this paragraph)

Exhibit A
Program Specifications

- ii. MHSa Quarterly Progress Reports, as specified in the California Code of Regulations. Title 9, section 3530.20. MHSa Quarterly Progress Reports provide the actual number of clients served by MHSa-funded program. Reports are submitted on a quarterly basis.
 - iii. Full Service Partnership Performance Outcome data, as specified in the California Code of Regulations, Title 9, section 3530.30.
 - iv. Consumer Perception Survey data, as specified in the California Code of Regulations, Title 9, section 3530.40.
 - v. The Annual Mental Health Services Act Revenue and Expenditure Report, as specified in Welfare and Institutions Code section 5899(a) and the California Code of Regulations, Title 9, sections 3510, 3510.010, and 3510.020 and DHCS-issued guidelines.
 - vi. Innovative Project Reports (annual, final and supplements), as specified in the California Code of Regulations, Title 9, sections 3580 through 3580.02.
 - vii. The Annual Prevention and Early Intervention report, as specified in the California Code of Regulations, Title 9, sections 3560 and 3560.010.
 - viii. Three Year Program and Evaluation Reports, as specified in the California Code of Regulations, Title 9, sections 3560 and 3560.020.
- C. County shall submit CSI data to DHCS, in accordance with Title 9 of the California Code of Regulations, section 3530.10, and according to the specifications set for in DHCS' CSI Data Dictionary, County shall:
- i. Report monthly CSI data to DHCS within 60 calendar days after the end of the month in which services were provided.
 - ii. Report within 60 calendar days or be in compliance with an approved plan of correction to the DHCS's CSI Unit.
 - iii. Make diligent efforts to minimize errors on the CSI error file.
 - iv. Notify DHCS 90 calendar days prior to any change in reporting system and/or change of automated system vendor.
- a. In the event that DHCS or County determines that, due to federal or state law changes or business requirements, an amendment is needed of either County's or DHCS' obligations under this contract relating to either DHCS' or County's information needs both DHCS and County agree to provide notice to the other party as soon as practicable prior to implementation. This notice shall include information and comments regarding the anticipated requirements and impacts of

Exhibit A
Program Specifications

the projected changes. DHCS and County agree to meet and discuss the design, development, and costs of the anticipated changes prior to implementation.

- b. For all mental health funding sources received by County that require submission of a cost report, County shall submit a fiscal year-end cost report by December 31 following the close of the fiscal year in accordance with applicable federal and State law, regulations and DHCS-issued guidelines. (Welf. & Inst. Code § 5705; Cal. Code Regs., tit. 9, §§ 3500, 3505.) The cost report shall be certified as true and correct, and with respect to Mental Health Service Fund moneys, that the County is in compliance with the California Code of Regulations, Title 9, section 3410, Non-Supplant. The certification must be completed by the mental health director and one of the following: the County mental health departments chief financial officer (or equivalent), and individual who has delegated authority to sign for, and reports directly to the county mental health department's chief financial officer (or equivalent), or the county's auditor-controller (or equivalent). Data submitted shall be full and complete. The County shall also submit a reconciled cost report certified by the mental health director and the county's auditor-controller as being true and correct no later than 18 months after the close of the following fiscal year.
- c. If applicable to a specific federal or state funding source covered by this Agreement, County shall require each of its subcontractors to submit a fiscal year-end cost report to DHCS no later than December 31 following the close of the fiscal year, in accordance with applicable federal and state laws, regulations, and DHCS-issued guidelines.

8. Special Terms and Conditions

A. Audit and Record Retention

(Applicable to agreements in excess of \$10,000)

- 1) County and/or Subcontractor(s) shall maintain records, including books,, documents, and other evidence, accounting procedures and practices, sufficient to properly support all direct and indirect costs of whatever nature claimed to have been incurred in the performance of this Agreement, including any matching costs and expenses. The forgoing constitutes "records" for the purpose of this provision.
- 2) County's and/or Subcontractor's facility or office or such part thereof as may be engaged in the performance of this Agreement and his/her records shall be subject at all reasonable times to inspection, audit, and reproduction.
- 3) County agrees that DHCS, the Department of General Services, the Bureau of State Audits, or their designated representatives including the Comptroller General of the United States shall have the right to review and copy any records and supporting documentation pertaining to the performance of this Agreement.

Exhibit A
Program Specifications

County agrees to allow the auditor(s) access to such records during normal business hours and to allow interviews of any employees who might reasonably have information related to such records. Further, County agrees to include a similar right of the State to audit records and interview staff in any subcontract related to performance of this Agreement.

- 4) County and/or Subcontractor(s) shall preserve and make available his/her records (1) for a period of ten years from the date of final payment under this Agreement, and (2) for such longer period, if any, as is required by applicable statute, by any other provision of this Agreement, or by subparagraphs (a) or (b) below.
 - a. If this Agreement is completely or partially terminated, the records relating to the work terminated shall be preserved and made available for a period of three years from the date of any resulting final settlement.
 - b. If any litigation, claim, negotiation, audit, or other action involving the records has been started before the expiration of the ten-year period, the records shall be retained until completion of the action and resolution of all issues which arise from it, or until the end of the regular ten-year period, whichever is later.
- 5) County and/or Subcontractor(s) may, at its discretion, following receipt of final payment under this Agreement, reduce its accounts, books, and records related to this Agreement to microfilm, computer disk, CD ROM, DVD, or other data storage medium. Upon request by an authorized representative to inspect, audit or obtain copies of said records, County and/or Subcontractor(s) must supply or make available applicable devices, hardware, and/or software necessary to view, copy, and/or print said records. Applicable devices may include, but are not limited to, microfilm readers and microfilm printers, etc.
- 6) County shall, if applicable, comply with the Single Audit Act and the audit reporting requirements set forth in 2 Code of Regulations part 200.

B. Dispute Resolution Process for Projects for Assistance in Transition from Homelessness Program Grant and Community Mental Health Services Grant Program

If a dispute arises between the Contractor and DHCS regarding Contractor compliance with Section 6, of this Agreement, subsection B, Projects for Assistance in Transition from Homelessness Program or subsection C, Community Mental Health Services Grant Program, the Contractor must seek resolution using the process outlined below.

- 1) The Contractor must first informally discuss the problem with the DHCS Project Representative listed in paragraph 3. If the parties are unable to resolve the problem informally, the Contractor must mail a written Statement of Dispute, with supporting evidence, to DHCS at the address listed in paragraph 3 below. The

Exhibit A
Program Specifications

Statement of Dispute must describe the issues in dispute, the legal authority or other basis for the Contractor's position, and the remedy sought.

- 2) The Branch Chief of DHCS' Mental Health Management and Outcomes Reporting Branch will decide the dispute and mail a written decision to the Contractor within twenty (20) working days of receiving the Statement of Dispute from the Contractor. The decision will be in writing, resolve the dispute and include a statement of the reasons for the decision that addresses each issue raised by the Contractor. If applicable, the decision will also indicate any action Contractor must take to comply with the decision. The Branch Chief's decision shall be the final administrative determination of DHCS.
- 3) Unless otherwise agreed to in writing by DHCS, the Statement of Dispute, supporting documentation, and all correspondence and documents related to the dispute resolution process shall be directed to the following:

Department of Health Care Services
Mental Health Services Division/Program Policy Unit
Attention: Guy Stewart
1500 Capitol Avenue, MS 2702
P.O. Box Number 997413
Sacramento, CA, 95899-7413

C. Novation

If County proposes any novation agreement, DHCS shall act upon the proposal within 60 days after receipt of the written proposal. DHCS may review and consider the proposal, consult and negotiate with County, and accept or reject all or part of the proposal. Acceptance or rejection of the proposal may be made orally within the 60-day period and confirmed in writing within five days of said decision. Upon written acceptance of the proposal, DHCS will initiate an amendment to this Agreement to formally implement the approved proposal.

D. Laura's Law

If County chooses to participate in the Assisted Outpatient Treatment program (AOT) Demonstration Project Act of 2002 it shall be required to comply with all applicable statutes including, but not limited to, Welfare and Institutions Code sections 5345 through 5349.5, inclusive. In addition, County shall submit to DHCS any documents that DHCS requests as part of its statutory responsibilities in accordance with DMH Letter No.: 03-01 dated March 20, 2003.

E. Welfare and Institutions Code section 5751.7 Waiver

- 1) County shall comply with Welfare and Institutions Code section 5751.7 and ensure that minors are not admitted into inpatient psychiatric treatment with adults. If this requirement creates undue hardship to County due to inadequate

Exhibit A
Program Specifications

or unavailable alternative resources, County may request a waiver of this requirement. County shall submit the waiver request on Attachment I of this Agreement, to DHCS.

- 2) DHCS shall review County's waiver request and provide a written notice of approval or denial of the waiver. If County's waiver request is denied, County shall prohibit health facilities from admitting minors into psychiatric treatment with adults.
- 3) County shall submit, the waiver request to DHCS at the time County submits this Agreement, signed by County, to DHCS for execution. County shall complete Attachment I, and attach it to this Agreement. See Exhibit A, Attachment I, entitled "Request For Waiver" of this Agreement for additional submission information.
Execution of this Agreement by DHCS shall not constitute approval of a waiver submitted pursuant to this section.
Any waiver granted in the prior fiscal year's Agreement shall be deemed to continue until either party chooses to discontinue it, as specified in Exhibit A, Attachment I. Execution of this Agreement shall continue independently of the waiver review and approval process.
- 4) In unusual or emergency circumstances, when County needs to request waivers after the annual Performance Contract has been executed, these requests should be sent immediately to: Licensing and Certification Section, Program Oversight and Compliance Branch, California Department of Health Care Services, P.O. Box 997413, MS 2800, Sacramento, CA 95899-7413, telephone: (916) 323-1864.
- 5) Each admission of a minor to a facility that has an approved waiver shall be reported to the Local Mental Health Director.

F. Americans with Disabilities Act

Contractor agrees to ensure that deliverables developed and produced, pursuant to this Agreement shall comply with the accessibility requirements of Section 508 of the Rehabilitation Act and the Americans with Disabilities Act of 1973 as amended (29 U.S.C. § 794 (d)), and regulations implementing that Act as set forth in Part 1194 of Title 36 of the Code of Federal Regulations. In 1998, Congress amended the Rehabilitation Act of 1973 to require Federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities. California Government Code section 11135 codifies section 508 of the Act requiring accessibility of electronic and information technology.

Exhibit A, Attachment I
Request for Waiver

Request for Waiver Pursuant To Section 5751.7 of the Welfare and Institutions Code

_____ hereby requests a waiver for the following public or private health facilities pursuant to section 5751.7 of the Welfare and Institutions Code for the term of this contract. These are facilities where minors may be provided psychiatric treatment with nonspecific separate housing arrangements, treatment staff, and treatment programs designed to serve minors. However, no minor shall be admitted for psychiatric treatment into the same treatment ward as an adult receiving treatment who is in the custody of any jailor for a violent crime, is a known registered sex offender, or has a known history of, or exhibits inappropriate sexual or other violent behavior which would present a threat to the physical safety of others.

The request for waiver must include, as an attachment, the following:

1. A description of the hardship to the County/City due to inadequate or unavailable alternative resources that would be caused by compliance with the state policy regarding the provision of psychiatric treatment to minors.
2. The specific treatment protocols and administrative procedures established by the County/City for identifying and providing appropriate treatment to minors admitted with adults.
3. Name, address, and telephone number of the facility
 - Number of the facility's beds designated for involuntary treatment
 - Type of facility, license(s), and certification(s) held (including licensing and certifying agency and license and certificate number)
 - A copy of the facility's current license or certificate and description of the program, including target population and age groups to be admitted to the designated facility.
4. If applicable, the County Board of Supervisors' decision to designate a facility as a facility for evaluation and treatment pursuant to Welfare and Institutions Code sections 5150, 5585.50, and 5585.55.

To rescind the a waiver, either party shall send a letter to the other party on official letterhead signed by their respective Behavioral Health Director or his or her designee indicating that the party no longer grants or requests a waiver. If not otherwise specified by the party in the letter to the respective party, the discontinuance shall be effective the date the letter to the party is postmarked and the facility shall no longer be waived as of this date.

When the Department denies or rescinds a waiver issued to a County, the facility and the County Behavioral Health Director or designee shall receive written notification from the Department, by certified mail or e-mail. The notice shall include the decision, the basis for the decision, and any supporting documentation.

**Exhibit B
Funds Provision**

1. Budget Contingency Clause

- A. It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Agreement does not appropriate sufficient funds for the program, this Agreement shall be of no further force and effect. In this event, DHCS shall have no liability to pay any funds whatsoever to Inyo County Mental Health or to furnish any other considerations under this Agreement and Imperial Inyo County Mental Health shall not be obligated to perform any provisions of this Agreement.

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

Exhibit D
Information Confidentiality and Security Requirements

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 6250-6265) 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 6250-6265) 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 DHCS' policy to consider all information about individuals private unless such information is determined to be a public record.** This information must be protected from inappropriate access, use, or disclosure and must 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 DHCS Program 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 DHCS without prior written authorization from the DHCS Program Contract Manager, except if disclosure is required by State or Federal law.

Exhibit D
Information Confidentiality and Security Requirements

6. The Contractor shall observe the following requirements:

A. Safeguards. The Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PSCI, including electronic PSCI that it creates, receives, maintains, uses, or transmits on behalf of DHCS. Contractor shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities, 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 DHCS, or access or disclose DHCS PSCI, must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.
- b. Employee Discipline.** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
- c. Confidentiality Statement.** All persons that will be working with DHCS PSCI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to DHCS PSCI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for DHCS inspection for a period of six (6) years following contract termination.
- d. Background Check.** Before a member of the workforce may access DHCS PSCI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

2) Technical Security Controls

- a. Workstation/Laptop encryption.** All workstations and laptops that process and/or store DHCS PSCI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the DHCS Information Security Office.
- b. Server Security.** Servers containing unencrypted DHCS PSCI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

Exhibit D
Information Confidentiality and Security Requirements

- c. **Minimum Necessary.** Only the minimum necessary amount of DHCS PSCI required to perform necessary business functions may be copied, downloaded, or exported.
- d. **Removable media devices.** All electronic files that contain DHCS PSCI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smartphones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.
- e. **Antivirus software.** All workstations, laptops and other systems that process and/or store DHCS PSCI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.
- f. **Patch Management.** All workstations, laptops and other systems that process and/or store DHCS PSCI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.
- g. **User IDs and Password Controls.** All users must be issued a unique user name for accessing DHCS PSCI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:
- Upper case letters (A-Z)
 - Lower case letters (a-z)
 - Arabic numerals (0-9)
 - Non-alphanumeric characters (punctuation symbols)
- h. **Data Destruction.** When no longer needed, all DHCS PSCI must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PSCI cannot be retrieved.
- i. **System Timeout.** The system providing access to DHCS PSCI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.
- j. **Warning Banners.** All systems providing access to DHCS PSCI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.
- k. **System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DHCS PSCI, or which alters DHCS PSCI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If DHCS PSCI is

Exhibit D
Information Confidentiality and Security Requirements

stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

- l. Access Controls.** The system providing access to DHCS PSCI must use role based access controls for all user authentications, enforcing the principle of least privilege.
- m. Transmission encryption.** All data transmissions of DHCS PSCI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PSCI can be encrypted. This requirement pertains to any type of PSCI in motion such as website access, file transfer, and E-Mail.
- n. Intrusion Detection.** All systems involved in accessing, holding, transporting, and protecting DHCS PSCI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3) Audit Controls

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

4) Business Continuity / Disaster Recovery Controls

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

5) Paper Document Controls

- a. Supervision of Data.** DHCS PSCI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information.

Exhibit D
Information Confidentiality and Security Requirements

DHCS 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 DHCS PSCI is contained shall be escorted and DHCS PSCI shall be kept out of sight while visitors are in the area.
 - c. **Confidential Destruction.** DHCS PSCI must be disposed of through confidential means, such as cross cut shredding and pulverizing.
 - d. **Removal of Data.** DHCS PSCI must not be removed from the premises of the Contractor except with express written permission of DHCS.
 - e. **Faxing.** Faxes containing DHCS 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 the fax.
 - f. **Mailing.** Mailings of DHCS PSCI shall be sealed and secured from damage or inappropriate viewing of PSCI to the extent possible. Mailings which include 500 or more individually identifiable records of DHCS PSCI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of DHCS to use another method is obtained.
- B. 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 DHCS.

Discovery and Notification of Breach. Notice to DHCS:

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

Notice shall be provided to the DHCS Program Contract Manager, the DHCS Privacy Officer and the DHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves data provided to DHCS by the Social Security Administration, notice shall be provided by calling the DHCS EITS Service Desk. Notice shall be made using the "DHCS Privacy Incident Report" form, including all information known at the time. The contractor shall use the most current version of this form, which is posted on the DHCS Privacy Office website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Use" near the middle of the page) or use this link: <http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx>

Exhibit D
Information Confidentiality and Security Requirements

- C. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PSCI, the Contractor shall take:
- 1) Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment and
 - 2) Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
- D. **Investigation of Breach.** The Contractor shall immediately investigate such security incident, breach, or unauthorized use or disclosure of PSCI. If the initial report did not include all of the requested information marked with an asterisk, then within seventy-two (72) hours of the discovery, The Contractor shall submit an updated "DHCS Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer:
- E. **Written Report.** The Contractor shall provide a written report of the investigation to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer, if all of the required information was not included in the DHCS Privacy Incident Report, within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. 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.
- F. **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 DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS 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 contracts, 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 DHCS staff, the Contractor shall initiate contact as indicated herein. DHCS 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.

DHCS Program Contract Manager	DHCS Privacy Officer	DHCS Information Security Officer
----------------------------------	----------------------	-----------------------------------

Exhibit D
Information Confidentiality and Security Requirements

See the Scope of Work exhibit for Program Contract Manager information	Privacy Officer c/o Office of Legal Services Department of Health Care Services P.O. Box 997413, MS 0011 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Telephone: ITSD Help Desk (916) 440-7000 or (800) 579-0874
--	--	--

9. **Audits and Inspections.** From time to time, DHCS 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. Contractor shall promptly remedy any violation of any provision of this ICSR exhibit. The fact that DHCS inspects, or fails to inspect, or has the right to inspect, Contractor's facilities, systems and procedures does not relieve Contractor of its responsibility to comply with this ICSR exhibit.

EXHIBIT E

PRIVACY AND INFORMATION SECURITY PROVISIONS

This Exhibit E is intended to protect the privacy and security of specified Department information that Contractor may access, receive, or transmit under this Agreement. The Department information covered under this Exhibit E consists of: (1) Protected Health Information as defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA")(PHI); and (2) Personal Information (PI) as defined under the California Information Practices Act (CIPA), at California Civil Code Section 1798.3. Personal Information may include data provided to the Department by the Social Security Administration.

Exhibit E consists of the following parts:

1. Exhibit E-1, HIPAA Business Associate Addendum, which provides for the privacy and security of PHI.
2. Exhibit E-2, which provides for the privacy and security of PI in accordance with specified provisions of the Agreement between the Department and the Social Security Administration, known as the Information Exchange Agreement (IEA) and the Computer Matching and Privacy Protection Act Agreement between the Social Security Administration and the California Health and Human Services Agency (Computer Agreement) to the extent Contractor access, receives, or transmits PI under these Agreements. Exhibit E-2 further provides for the privacy and security of PI under Civil Code Section 1798.3(a) and 1798.29.
3. Exhibit E-3, Miscellaneous Provision, sets forth additional terms and conditions that extend to the provisions of Exhibit E in its entirety.

EXHIBIT E-1

HIPAA Business Associate Addendum

1. Recitals.

- A. A business associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), 42 U.S.C. Section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations") between Department and Contractor arises only to the extent that Contractor creates, receives, maintains, transmits, uses or discloses PHI or ePHI on the Department's behalf, or provides services, arranges, performs or assists in the performance of functions or activities on behalf of the Department that are included in the definition of "business associate" in 45 C.F.R. 160.103 where the provision of the service involves the disclosure of PHI or ePHI from the Department, including but not limited to, utilization review, quality assurance, or benefit management. To the extent Contractor performs these services, functions, and activities on behalf of Department, Contractor is the Business Associate of the Department, acting on the Department's behalf. The Department and Contractor are each a party to this Agreement and are collectively referred to as the "parties."
- B. The Department wishes to disclose to Contractor certain information pursuant to the terms of this Agreement, some of which may constitute Protected Health Information ("PHI"), including protected health information in electronic media ("ePHI"), under federal law, to be used or disclosed in the course of providing services and activities as set forth in Section 1.A. of Exhibit E-1 of this Agreement. This information is hereafter referred to as "Department PHI".
- C. The purpose of this Exhibit E-1 is to protect the privacy and security of the PHI and ePHI that may be created, received, maintained, transmitted, used or disclosed pursuant to this Agreement, and to comply with certain standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations, including, but not limited to, the requirement that the Department must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 CFR Parts 160 and 164 and the HITECH

Act. To the extent that data is both PHI or ePHI and Personally Identifying Information, both Exhibit E-2 (including Attachment B, the SSA Agreement between SSA, CHHS and DHCS, referred to in Exhibit E-2) and this Exhibit E-1 shall apply.

- D. The terms used in this Exhibit E-1, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

2. Definitions.

- A. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- B. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- C. Covered Entity shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- D. Department PHI shall mean Protected Health Information or Electronic Protected Health Information, as defined below, accessed by Contractor in a database maintained by the Department, received by Contractor from the Department or acquired or created by Contractor in connection with performing the functions, activities and services on behalf of the Department as specified in Section 1.A. of Exhibit E-1 of this Agreement. The terms PHI as used in this document shall mean Department PHI.
- E. Electronic Health Records shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921 and implementing regulations.
- F. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 CFR section 160.103.
- G. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual

or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 CFR Section 160.103.

- H. Privacy Rule shall mean the HIPAA Regulations that are found at 45 CFR Parts 160 and 164, subparts A and E.
- I. Protected Health Information (PHI) means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR Section 160.103 and as defined under HIPAA.
- J. Required by law, as set forth under 45 CFR Section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
- K. Secretary means the Secretary of the U.S. Department of Health and Human Services ("HHS") or the Secretary's designee.
- L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of Department PHI, or confidential data utilized by Contractor to perform the services, functions and activities on behalf of Department as set forth in Section 1.A. of Exhibit E-1 of this Agreement; or interference with system operations in an information system that processes, maintains or stores Department PHI.
- M. Security Rule shall mean the HIPAA regulations that are found at 45 CFR Parts 160 and 164.
- N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. Section 17932(h), any guidance issued by the Secretary pursuant to such Act and the HIPAA regulations.

3. Terms of Agreement.

A. Permitted Uses and Disclosures of Department PHI by Contractor.

Except as otherwise indicated in this Exhibit E-1, Contractor may use or disclose Department PHI only to perform functions, activities or services specified in Section 1.A of Exhibit E-1 of this Agreement, for, or on behalf of the Department, provided that such use or disclosure would not violate the HIPAA regulations or the limitations set forth in 42 CFR Part 2, or any other applicable law, if done by the Department. Any such use or disclosure, if not for purposes of treatment activities of a health care provider as defined by the Privacy Rule, must, to the extent practicable, be limited to the limited data set, as defined in 45 CFR Section 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, and the HIPAA regulations.

B. Specific Use and Disclosure Provisions. Except as otherwise indicated in this Exhibit E-1, Contractor may:

- 1) **Use and Disclose for Management and Administration.** Use and disclose Department PHI for the proper management and administration of the Contractor's business, provided that such disclosures are required by law, or the Contractor obtains reasonable assurances from the person to whom the information is disclosed, in accordance with section D(7) of this Exhibit E-1, that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Contractor of any instances of which it is aware that the confidentiality of the information has been breached.
- 2) **Provision of Data Aggregation Services.** Use Department PHI to provide data aggregation services to the Department to the extent requested by the Department and agreed to by Contractor. Data aggregation means the combining of PHI created or received by the Contractor, as the Business Associate, on behalf of the Department with PHI received by the Business Associate in its capacity as the Business Associate of another covered entity, to permit data analyses that relate to the health care operations of the Department

C. Prohibited Uses and Disclosures

- 1) Contractor shall not disclose Department PHI about an individual to a health plan for payment or health care operations purposes if the Department PHI pertains solely to a health care item or service for

which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. Section 17935(a) and 45 CFR Section 164.522(a).

- 2) Contractor shall not directly or indirectly receive remuneration in exchange for Department PHI.

D. Responsibilities of Contractor

Contractor agrees:

- 1) **Nondisclosure.** Not to use or disclose Department PHI other than as permitted or required by this Agreement or as required by law, including but not limited to 42 CFR Part 2.
- 2) **Compliance with the HIPAA Security Rule.** To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Department PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of the Department, in compliance with 45 CFR Sections 164.308, 164.310 and 164.312, and to prevent use or disclosure of Department PHI other than as provided for by this Agreement. Contractor shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR Section 164, subpart C, in compliance with 45 CFR Section 164.316. Contractor shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities, and which incorporates the requirements of section 3, Security, below. Contractor will provide the Department with its current and updated policies upon request.
- 3) **Security.** Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:
 - a. Complying with all of the data system security precautions listed in Attachment A, Data Security Requirements;
 - b. Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of DHCS under this

Agreement; and

- c. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies.
- 4) **Security Officer.** Contractor shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with the Department.
 - 5) **Mitigation of Harmful Effects.** To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Department PHI by Contractor or its subcontractors in violation of the requirements of this Exhibit E.
 - 6) **Reporting Unauthorized Use or Disclosure.** To report to Department any use or disclosure of Department PHI not provided for by this Exhibit E of which it becomes aware.
 - 7) **Contractor's Agents and Subcontractors.**
 - a. To enter into written agreements with any agents, including subcontractors and vendors to whom Contractor provides Department PHI, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Contractor with respect to such Department PHI under this Exhibit E, and that require compliance with all applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, including the requirement that any agents, subcontractors or vendors implement reasonable and appropriate administrative, physical, and technical safeguards to protect such PHI. As required by HIPAA, the HITECH Act and the HIPAA regulations, including 45 CFR Sections 164.308 and 164.314, Contractor shall incorporate, when applicable, the relevant provisions of this Exhibit E-1 into each subcontract or subaward to such agents, subcontractors and vendors, including the requirement that any security incidents or breaches of unsecured PHI be reported to Contractor.
 - b. In accordance with 45 CFR Section 164.504(e)(1)(ii), upon

Contractor's knowledge of a material breach or violation by its subcontractor of the agreement between Contractor and the subcontractor, Contractor shall:

- i) Provide an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by the Department; or
- ii) Immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.

8) Availability of Information to the Department and Individuals to Provide Access and Information:

- a. To provide access as the Department may require, and in the time and manner designated by the Department (upon reasonable notice and during Contractor's normal business hours) to Department PHI in a Designated Record Set, to the Department (or, as directed by the Department), to an Individual, in accordance with 45 CFR Section 164.524. Designated Record Set means the group of records maintained for the Department health plan under this Agreement that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for the Department health plan for which Contractor is providing services under this Agreement; or those records used to make decisions about individuals on behalf of the Department. Contractor shall use the forms and processes developed by the Department for this purpose and shall respond to requests for access to records transmitted by the Department within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.
- b. If Contractor maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Contractor shall provide such information in an electronic format to enable the Department to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. Section 17935(e) and the HIPAA regulations.

- 9) **Amendment of Department PHI.** To make any amendment(s) to Department PHI that were requested by a patient and that the Department directs or agrees should be made to assure compliance with 45 CFR Section 164.526, in the time and manner designated by the Department, with the Contractor being given a minimum of twenty (20) days within which to make the amendment.
- 10) **Internal Practices.** To make Contractor's internal practices, books and records relating to the use and disclosure of Department PHI available to the Department or to the Secretary, for purposes of determining the Department's compliance with the HIPAA regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Contractor, Contractor shall provide written notification to the Department and shall set forth the efforts it made to obtain the information.
- 11) **Documentation of Disclosures.** To document and make available to the Department or (at the direction of the Department) to an individual such disclosures of Department PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of such PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 CFR Section 164.528 and 42 U.S.C. Section 17935(c). If Contractor maintains electronic health records for the Department as of January 1, 2009 and later, Contractor must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting.
- 12) **Breaches and Security Incidents.** During the term of this Agreement, Contractor agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:
 - a. **Initial Notice to the Department.** (1) To notify the Department **immediately by telephone call or email or fax** upon the discovery of a breach of unsecured PHI in electronic media or in any other media if the PHI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person. (2) To notify the Department **within 24 hours (one hour if SSA data) by email or fax** of

the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI in violation of this Agreement or this Exhibit E-1, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Contractor.

Notice shall be provided to the Information Protection Unit, Office of HIPAA Compliance. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notice shall be provided by calling the Information Protection Unit (916.445.4646, 866-866-0602) or by emailing privacyofficer@dhcs.ca.gov). Notice shall be made using the DHCS "Privacy Incident Report" form, including all information known at the time. Contractor shall use the most current version of this form, which is posted on the DHCS Information Security Officer website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Partner" near the middle of the page) or use this link:

<http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx>

Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of Department PHI, Contractor shall take:

- i) Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
 - ii) Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
- b. **Investigation and Investigation Report.** To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI. Within 72 hours of the discovery, Contractor shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the

form, to the extent known at that time, to the Information Protection Unit.

- c. **Complete Report.** To provide a complete report of the investigation to the Department Program Contract Manager and the Information Protection Unit within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, and the HIPAA regulations. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the Department requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the Department with such information. If, because of the circumstances of the incident, Contractor needs more than ten (10) working days from the discovery to submit a complete report, the Department may grant a reasonable extension of time, in which case Contractor shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. The Department will review and approve the determination of whether a breach occurred and whether individual notifications and a corrective action plan are required.
- d. **Responsibility for Reporting of Breaches.** If the cause of a breach of Department PHI is attributable to Contractor or its agents, subcontractors or vendors, Contractor is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary (after obtaining prior written approval of DHCS). If a breach of unsecured Department PHI involves more than 500 residents of the State of California or under its jurisdiction, Contractor shall first notify DHCS, then the Secretary of the breach immediately upon discovery of the breach. If a breach involves more than 500 California residents, Contractor shall also provide, after obtaining written prior approval of DHCS, notice to the Attorney General for the State of California,

Privacy Enforcement Section. If Contractor has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to the Department in addition to Contractor, Contractor shall notify the Department, and the Department and Contractor may take appropriate action to prevent duplicate reporting.

- e. **Responsibility for Notification of Affected Individuals.** If the cause of a breach of Department PHI is attributable to Contractor or its agents, subcontractors or vendors and notification of the affected individuals is required under state or federal law, Contractor shall bear all costs of such notifications as well as any costs associated with the breach. In addition, the Department reserves the right to require Contractor to notify such affected individuals, which notifications shall comply with the requirements set forth in 42U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days after discovery of the breach. The Department Privacy Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made. The Department will provide its review and approval expeditiously and without unreasonable delay.

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

Department Program Contract Manager	DHCS Privacy Officer	DHCS Information Security Officer
--	-----------------------------	--

<p>See the Exhibit A, Scope of Work for Program Contract Manager information</p>	<p>Information Protection Unit c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 (916) 445-4646; (866) 866-0602</p> <p>Email: privacyofficer@dhcs.ca.gov</p> <p>Fax: (916) 440-7680</p>	<p>Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413</p> <p>Email: iso@dhcs.ca.gov</p> <p>Telephone: ITSD Service Desk (916) 440-7000; (800) 579-0874</p> <p>Fax: (916)440-5537</p>
--	--	--

- 13) **Termination of Agreement.** In accordance with Section 13404(b) of the HITECH Act and to the extent required by the HIPAA regulations, if Contractor knows of a material breach or violation by the Department of this Exhibit E-1, it shall take the following steps:
- a. Provide an opportunity for the Department to cure the breach or end the violation and terminate the Agreement if the Department does not cure the breach or end the violation within the time specified by Contractor; or
 - b. Immediately terminate the Agreement if the Department has breached a material term of the Exhibit E-1 and cure is not possible.
- 14) **Sanctions and/or Penalties.** Contractor understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to Contractors may result in the imposition of sanctions and/or penalties on Contractor under HIPAA, the HITECH Act and the HIPAA regulations.

E. Obligations of the Department.

The Department agrees to:

- 1) **Permission by Individuals for Use and Disclosure of PHI.** Provide the Contractor with any changes in, or revocation of, permission by an Individual to use or disclose Department PHI, if such changes affect the Contractor's permitted or required uses and disclosures.
- 2) **Notification of Restrictions.** Notify the Contractor of any restriction to

the use or disclosure of Department PHI that the Department has agreed to in accordance with 45 CFR Section 164.522, to the extent that such restriction may affect the Contractor's use or disclosure of PHI.

- 3) **Requests Conflicting with HIPAA Rules.** Not request the Contractor to use or disclose Department PHI in any manner that would not be permissible under the HIPAA regulations if done by the Department.
- 4) **Notice of Privacy Practices.** Provide Contractor with the web link to the Notice of Privacy Practices that DHCS produces in accordance with 45 CFR Section 164.520, as well as any changes to such notice. Visit the DHCS website to view the most current Notice of Privacy Practices at:
<http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/NoticeofPrivacyPractices.aspx> or the DHCS website at www.dhcs.ca.gov (select "Privacy in the right column and "Notice of Privacy Practices" on the right side of the page).

F. Audits, Inspection and Enforcement

If Contractor is the subject of an audit, compliance review, or complaint investigation by the Secretary or the Office for Civil Rights, U.S. Department of Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Exhibit E-1, Contractor shall immediately notify the Department. Upon request from the Department, Contractor shall provide the Department with a copy of any Department PHI that Contractor, as the Business Associate, provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI to the Secretary. Contractor is responsible for any civil penalties assessed due to an audit or investigation of Contractor, in accordance with 42 U.S.C. Section 17934(c).

G. Termination.

- 1) **Term.** The Term of this Exhibit E-1 shall extend beyond the termination of the Agreement and shall terminate when all Department PHI is destroyed or returned to the Department, in accordance with 45 CFR Section 164.504(e)(2)(ii)(J).
- 2) **Termination for Cause.** In accordance with 45 CFR Section 164.504(e)(1)(iii), upon the Department's knowledge of a material breach or violation of this Exhibit E-1 by Contractor, the Department shall:
 - a. Provide an opportunity for Contractor to cure the breach or

end the violation and terminate this Agreement if Contractor does not cure the breach or end the violation within the time specified by the Department; or

- b. Immediately terminate this Agreement if Contractor has breached a material term of this Exhibit E-1 and cure is not possible.

THE REST OF THIS PAGE IS INTENTIONALLY BLANK

EXHIBIT E-2

Privacy and Security of Personal Information and Personally Identifiable Information Not Subject to HIPAA

1. Recitals.

- A. In addition to the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) the Department is subject to various other legal and contractual requirements with respect to the personal information (PI) and personally identifiable information (PII) it maintains. These include:
- 1) The California Information Practices Act of 1977 (California Civil Code §§1798 et seq.),
 - 2) The Agreement between the Social Security Administration (SSA) and the Department, known as the Information Exchange Agreement (IEA), which incorporates the Computer Matching and Privacy Protection Act Agreement (CMPPA) between the SSA and the California Health and Human Services Agency. The IEA, including the CMPPA is attached to this Exhibit E as Attachment B and is hereby incorporated in this Agreement.
 - 3) Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2.
- B. The purpose of this Exhibit E-2 is to set forth Contractor's privacy and security obligations with respect to PI and PII that Contractor may create, receive, maintain, use, or disclose for or on behalf of Department pursuant to this Agreement. Specifically this Exhibit applies to PI and PII which is not Protected Health Information (PHI) as defined by HIPAA and therefore is not addressed in Exhibit E-1 of this Agreement, the HIPAA Business Associate Addendum; however, to the extent that data is both PHI or ePHI and PII, both Exhibit E-1 and this Exhibit E-2 shall apply.
- C. The IEA Agreement referenced in A.2) above requires the Department to extend its substantive privacy and security terms to subcontractors who receive data provided to DHCS by the Social Security Administration. If Contractor receives data from DHCS that includes data provided to DHCS by the Social Security Administration, Contractor must comply with the following specific sections of the IEA Agreement: E. Security Procedures, F. Contractor/Agent Responsibilities, and G. Safeguarding and Reporting Responsibilities for Personally Identifiable Information ("PII"), and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local

Agencies Exchanging Electronic Information with the Social Security Administration. Contractor must also ensure that any agents, including a subcontractor, to whom it provides DHCS data that includes data provided by the Social Security Administration, agree to the same requirements for privacy and security safeguards for such confidential data that apply to Contractor with respect to such information.

- D. The terms used in this Exhibit E-2, but not otherwise defined, shall have the same meanings as those terms have in the above referenced statute and Agreement. Any reference to statutory, regulatory, or contractual language shall be to such language as in effect or as amended.

2. Definitions.

- A. "Breach" shall have the meaning given to such term under the IEA and CMPPA. It shall include a "PII loss" as that term is defined in the CMPPA.
- B. "Breach of the security of the system" shall have the meaning given to such term under the California Information Practices Act, Civil Code section 1798.29(f).
- C. "CMPPA Agreement" means the Computer Matching and Privacy Protection Act Agreement between the Social Security Administration and the California Health and Human Services Agency (CHHS).
- D. "Department PI" shall mean Personal Information, as defined below, accessed in a database maintained by the Department, received by Contractor from the Department or acquired or created by Contractor in connection with performing the functions, activities and services specified in this Agreement on behalf of the Department.
- E. "IEA" shall mean the Information Exchange Agreement currently in effect between the Social Security Administration (SSA) and the California Department of Health Care Services (DHCS).
- F. "Notice-triggering Personal Information" shall mean the personal information identified in Civil Code section 1798.29 whose unauthorized access may trigger notification requirements under Civil Code section 1798.29. For purposes of this provision, identity shall include, but not be limited to, name, address, email address, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, a photograph or a biometric identifier. Notice-triggering Personal Information includes PI in electronic, paper or any other medium.
- G. "Personally Identifiable Information" (PII) shall have the meaning given to such term in the IEA and CMPPA.

- H. "Personal Information" (PI) shall have the meaning given to such term in California Civil Code Section 1798.3(a).
- I. "Required by law" means a mandate contained in law that compels an entity to make a use or disclosure of PI or PII that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
- J. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PI, or confidential data utilized in complying with this Agreement; or interference with system operations in an information system that processes, maintains or stores PI.

3. Terms of Agreement

A. Permitted Uses and Disclosures of Department PI and PII by Contractor

Except as otherwise indicated in this Exhibit E-2, Contractor may use or disclose Department PI only to perform functions, activities or services for or on behalf of the Department pursuant to the terms of this Agreement provided that such use or disclosure would not violate the California Information Practices Act (CIPA) if done by the Department.

B. Responsibilities of Contractor

Contractor agrees:

- 1) **Nondisclosure.** Not to use or disclose Department PI or PII other than as permitted or required by this Agreement or as required by applicable state and federal law.
- 2) **Safeguards.** To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of Department PI and PII, to protect against anticipated threats or hazards to the security or

integrity of Department PI and PII, and to prevent use or disclosure of Department PI or PII other than as provided for by this Agreement. Contractor shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities, which incorporate the requirements of section 3, Security, below. Contractor will provide DHCS with its current policies upon request.

- 3) **Security.** Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:
- a. Complying with all of the data system security precautions listed in Attachment A, Business Associate Data Security Requirements;
 - b. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and
 - c. If the data obtained by Contractor from DHCS includes PII, Contractor shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between the SSA and DHCS, known as the Information Exchange Agreement, which are attached as Attachment B and incorporated into this Agreement. The specific sections of the IEA with substantive privacy and security requirements to be complied with are sections E, F, and G, and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the SSA. Contractor also agrees to ensure that any agents, including a subcontractor to whom it provides DHCS PII, agree to the same requirements for privacy and security safeguards for confidential data that apply to Contractor with respect to such information.

- 4) **Mitigation of Harmful Effects.** To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Department PI or PII by Contractor or its subcontractors in violation of this Exhibit E-2.
- 5) **Contractor's Agents and Subcontractors.** To impose the same restrictions and conditions set forth in this Exhibit E-2 on any subcontractors or other agents with whom Contractor subcontracts any activities under this Agreement that involve the disclosure of Department PI or PII to the subcontractor.
- 6) **Availability of Information to DHCS.** To make Department PI and PII available to the Department for purposes of oversight, inspection, amendment, and response to requests for records, injunctions, judgments, and orders for production of Department PI and PII. If Contractor receives Department PII, upon request by DHCS, Contractor shall provide DHCS with a list of all employees, contractors and agents who have access to Department PII, including employees, contractors and agents of its subcontractors and agents.
- 7) **Cooperation with DHCS.** With respect to Department PI, to cooperate with and assist the Department to the extent necessary to ensure the Department's compliance with the applicable terms of the CIPA including, but not limited to, accounting of disclosures of Department PI, correction of errors in Department PI, production of Department PI, disclosure of a security breach involving Department PI and notice of such breach to the affected individual(s).
- 8) **Confidentiality of Alcohol and Drug Abuse Patient Records.** Contractor agrees to comply with all confidentiality requirements set forth in Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2. Contractor is aware that criminal penalties may be imposed for a violation of these confidentiality requirements.
- 9) **Breaches and Security Incidents.** During the term of this Agreement, Contractor agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:
 - a. **Initial Notice to the Department.** (1) To notify the Department **immediately by telephone call or email or fax** upon the discovery of a breach of unsecured Department PI or PII in electronic media or in any other media if the PI or PII was, or is reasonably believed to have been, accessed or acquired

by an unauthorized person, or upon discovery of a suspected security incident involving Department PII. (2) To notify the Department **within one (1) hour by email or fax** if the data is data subject to the SSA Agreement; and **within 24 hours by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of Department PI or PII in violation of this Agreement or this Exhibit E-1 or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Contractor.

- b. Notice shall be provided to the Information Protection Unit, Office of HIPAA Compliance. If the incident occurs after business hours or on a weekend or holiday and involves electronic Department PI or PII, notice shall be provided by calling the Department Information Security Officer. Notice shall be made using the DHCS "Privacy Incident Report" form, including all information known at the time. Contractor shall use the most current version of this form, which is posted on the DHCS Information Security Officer website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Partner" near the middle of the page) or use this link:
<http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx> .
- c. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of Department PI or PII, Contractor shall take:
 - i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
 - ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
- d. **Investigation and Investigation Report.** To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of

PHI. Within 72 hours of the discovery, Contractor shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Department Information Security Officer.

- e. **Complete Report.** To provide a complete report of the investigation to the Department Program Contract Manager and the Information Protection Unit within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the Department requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the Department with such information. If, because of the circumstances of the incident, Contractor needs more than ten (10) working days from the discovery to submit a complete report, the Department may grant a reasonable extension of time, in which case Contractor shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. The Department will review and approve the determination of whether a breach occurred and whether individual notifications and a corrective action plan are required.
- f. **Responsibility for Reporting of Breaches.** If the cause of a breach of Department PI or PII is attributable to Contractor or its agents, subcontractors or vendors, Contractor is responsible for all required reporting of the breach as specified in CIPA, section 1798.29 and as may be required under the IEA. Contractor shall bear all costs of required notifications to individuals as well as any costs associated with the breach. The Privacy Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made. The Department will provide its review and approval expeditiously and without unreasonable delay.

- g. If Contractor has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to the Department in addition to Contractor, Contractor shall notify the Department, and the Department and Contractor may take appropriate action to prevent duplicate reporting.
- h. **Department Contact Information.** To direct communications to the above referenced Department staff, the Contractor shall initiate contact as indicated herein. The Department reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

Department Program Contract	DHCS Privacy Officer	DHCS Information Security Officer
See the Exhibit A, Scope of Work for Program Contract Manager information	Information Protection Unit c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 (916) 445-4646 Email: privacyofficer@dhcs.ca.gov Telephone:(916) 445-4646	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Telephone: ITSD Service Desk (916) 440-7000 or (800) 579-0874

10) Designation of Individual Responsible for Security

Contractor shall designate an individual, (e.g., Security Officer), to oversee its data security program who shall be responsible for carrying out the requirements of this Exhibit E-2 and for communicating on security matters with the Department.

EXHIBIT E-3

Miscellaneous Terms and Conditions

Applicable to Exhibit E

- 1) **Disclaimer.** The Department makes no warranty or representation that compliance by Contractor with this Exhibit E, HIPAA or the HIPAA regulations will be adequate or satisfactory for Contractor's own purposes or that any information in Contractor's possession or control, or transmitted or received by Contractor, is or will be secure from unauthorized use or disclosure. Contractor is solely responsible for all decisions made by Contractor regarding the safeguarding of the Department PHI, PI and PII.

- 2) **Amendment.** The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Exhibit E may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations, and other applicable state and federal laws. Upon either party's request, the other party agrees to promptly enter into negotiations concerning an amendment to this Exhibit E embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations, and other applicable state and federal laws. The Department may terminate this Agreement upon thirty (30) days written notice in the event:
 - a) Contractor does not promptly enter into negotiations to amend this Exhibit E when requested by the Department pursuant to this section; or
 - b) Contractor does not enter into an amendment providing assurances regarding the safeguarding of Department PHI that the Department deems is necessary to satisfy the standards and requirements of HIPAA and the HIPAA regulations.

- 3) **Judicial or Administrative Proceedings.** Contractor will notify the Department if it is named as a defendant in a criminal proceeding for a violation of HIPAA or other security or privacy law. The Department may terminate this Agreement if Contractor is found guilty of a criminal violation of HIPAA. The Department may terminate this Agreement if a finding or stipulation that the Contractor has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Contractor is a party or has been joined. DHCS will consider the nature and seriousness of the

- violation in deciding whether or not to terminate the Agreement.
- 4) **Assistance in Litigation or Administrative Proceedings.** Contractor shall make itself and any subcontractors, employees or agents assisting Contractor in the performance of its obligations under this Agreement, available to the Department at no cost to the Department to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Department, its directors, officers or employees based upon claimed violation of HIPAA, or the HIPAA regulations, which involves inactions or actions by the Contractor, except where Contractor or its subcontractor, employee or agent is a named adverse party.
 - 5) **No Third-Party Beneficiaries.** Nothing express or implied in the terms and conditions of this Exhibit E is intended to confer, nor shall anything herein confer, upon any person other than the Department or Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.
 - 6) **Interpretation.** The terms and conditions in this Exhibit E shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, and the HIPAA regulations. The parties agree that any ambiguity in the terms and conditions of this Exhibit E shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations, and, if applicable, any other relevant state and federal laws.
 - 7) **Conflict.** In case of a conflict between any applicable privacy or security rules, laws, regulations or standards the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI, PI and PII from unauthorized disclosure. Further, Contractor must comply within a reasonable period of time with changes to these standards that occur after the effective date of this Agreement.
 - 8) **Regulatory References.** A reference in the terms and conditions of this Exhibit E to a section in the HIPAA regulations means the section as in effect or as amended.
 - 9) **Survival.** The respective rights and obligations of Contractor under Section 3, Item D of Exhibit E-1, and Section 3, Item B of Exhibit E-2, Responsibilities of Contractor, shall survive the termination or expiration of this Agreement.
 - 10) **No Waiver of Obligations.** No change, waiver or discharge of any

liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

- 11) **Audits, Inspection and Enforcement.** From time to time, and subject to all applicable federal and state privacy and security laws and regulations, the Department may conduct a reasonable inspection of the facilities, systems, books and records of Contractor to monitor compliance with this Exhibit E. Contractor shall promptly remedy any violation of any provision of this Exhibit E. The fact that the Department inspects, or fails to inspect, or has the right to inspect, Contractor's facilities, systems and procedures does not relieve Contractor of its responsibility to comply with this Exhibit E. The Department's failure to detect a non-compliant practice, or a failure to report a detected non-compliant practice to Contractor does not constitute acceptance of such practice or a waiver of the Department's enforcement rights under this Agreement, including this Exhibit E.
- 12) **Due Diligence.** Contractor shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Exhibit E and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and other applicable state and federal law, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Exhibit E.
- 13) **Term.** The Term of this Exhibit E-1 shall extend beyond the termination of the Agreement and shall terminate when all Department PHI is destroyed or returned to the Department, in accordance with 45 CFR Section 164.504(e)(2)(ii)(I), and when all Department PI and PII is destroyed in accordance with Attachment A.
- 14) **Effect of Termination.** Upon termination or expiration of this Agreement for any reason, Contractor shall return or destroy all Department PHI, PI and PII that Contractor still maintains in any form, and shall retain no copies of such PHI, PI or PII. If return or destruction is not feasible, Contractor shall notify the Department of the conditions that make the return or destruction infeasible, and the Department and Contractor shall determine the terms and conditions under which Contractor may retain the PHI, PI or PII. Contractor shall continue to extend the protections of this Exhibit E to such Department PHI, PI and PII, and shall limit further use of such data to those purposes that make the return or destruction of such data infeasible. This provision shall apply to Department PHI, PI and PII that is in the possession of subcontractors or agents of Contractor.

Attachment A
Data Security Requirements

1. Personnel Controls

- A. **Employee Training.** All workforce members who assist in the performance of functions or activities on behalf of the Department, or access or disclose Department PHI or PI must complete information privacy and security training, at least annually, at Contractor's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following termination of this Agreement.
- B. **Employee Discipline.** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
- C. **Confidentiality Statement.** All persons that will be working with Department PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to Department PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for Department inspection for a period of six (6) years following termination of this Agreement.
- D. **Background Check.** Before a member of the workforce may access Department PHI or PI, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years.

2. Technical Security Controls

- A. **Workstation/Laptop encryption.** All workstations and laptops that store Department PHI or PI either directly or temporarily must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as

Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the Department Information Security Office.

- B. **Server Security.** Servers containing unencrypted Department PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
- C. **Minimum Necessary.** Only the minimum necessary amount of Department PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.
- D. **Removable media devices.** All electronic files that contain Department PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.
- E. **Antivirus software.** All workstations, laptops and other systems that process and/or store Department PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.
- F. **Patch Management.** All workstations, laptops and other systems that process and/or store Department PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release. Applications and systems that cannot be patched within this time frame due to significant operational reasons must have compensatory controls implemented to minimize risk until the patches can be installed. Applications and systems that cannot be patched must have compensatory controls implemented to minimize risk, where possible.
- G. **User IDs and Password Controls.** All users must be issued a unique user name for accessing Department PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed at least every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

- 1) Upper case letters (A-Z)

- 2) Lower case letters (a-z)
 - 3) Arabic numerals (0-9)
 - 4) Non-alphanumeric characters (punctuation symbols)
- H. **Data Destruction.** When no longer needed, all Department PHI or PI must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the Department Information Security Office.
- I. **System Timeout.** The system providing access to Department PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.
- J. **Warning Banners.** All systems providing access to Department PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.
- K. **System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for Department PHI or PI, or which alters Department PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If Department PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.
- L. **Access Controls.** The system providing access to Department PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.
- M. **Transmission encryption.** All data transmissions of Department PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing Department PHI can be encrypted. This requirement pertains to any type of Department PHI or PI in motion such as website access, file transfer, and E-Mail.
- N. **Intrusion Detection.** All systems involved in accessing, holding, transporting, and protecting Department PHI or PI that are accessible via

the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. Audit Controls

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

4. Business Continuity / Disaster Recovery Controls

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

5. Paper Document Controls

- A. **Supervision of Data.** Department PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. Department PHI or PI in

paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

- B. **Escorting Visitors.** Visitors to areas where Department PHI or PI is contained shall be escorted and Department PHI or PI shall be kept out of sight while visitors are in the area.
- C. **Confidential Destruction.** Department PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.
- D. **Removal of Data.** Only the minimum necessary Department PHI or PI may be removed from the premises of the Contractor except with express written permission of the Department. Department PHI or PI shall not be considered "removed from the premises" if it is only being transported from one of Contractor's locations to another of Contractor's locations.
- E. **Faxing.** Faxes containing Department PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.
- F. **Mailing.** Mailings containing Department PHI or PI shall be sealed and secured from damage or inappropriate viewing of such PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of Department PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of the Department to use another method is obtained.

**INFORMATION EXCHANGE AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION (SSA)
AND
THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES**

- A. PURPOSE:** The purpose of this Information Exchange Agreement (“IEA”) is to establish terms, conditions, and safeguards under which SSA will disclose to the State Agency certain information, records, or data (herein “data”) to assist the State Agency in administering certain federally funded, state-administered benefit programs (including state-funded, state supplementary payment programs under Title XVI of the Social Security Act) identified in this IEA. By entering into this IEA, the State Agency agrees to comply with:
- the terms and conditions set forth in the Computer Matching and Privacy Protection Act Agreement (“CMPPA Agreement”) attached as **Attachment 1**, governing the State Agency’s use of the data disclosed from SSA’s Privacy Act System of Records; and
 - all other terms and conditions set forth in this IEA and Attachments 2 through 6.
- B. PROGRAMS AND DATA EXCHANGE SYSTEMS:** (1) The State Agency will use the data received or accessed from SSA under this IEA for the purpose of administering the federally funded, state-administered programs identified in **Table 1** below. In **Table 1**, the State Agency has identified: (a) each federally funded, state-administered program that it administers; and (b) each SSA data exchange system to which the State Agency needs access in order to administer the identified program. The list of SSA’s data exchange systems is attached as **Attachment 2**. **Attachment 2** provides a brief explanation of each system, as well as use parameters, as necessary.

TABLE 1

FEDERALLY FUNDED BENEFIT PROGRAMS	
Program	SSA Data Exchange System(s)
<input checked="" type="checkbox"/> Medicaid	BENDEX/SDX/SVES IV/SOLQ/SVES-1-Citizenship/Quarters of Coverage/PUPS
<input type="checkbox"/> Temporary Assistance to Needy Families (TANF)	
<input type="checkbox"/> Supplemental Nutrition Assistance Program (SNAP- formally Food Stamps)	
<input type="checkbox"/> Unemployment Compensation	
<input type="checkbox"/> State Child Support Agency	
<input type="checkbox"/> Low-Income Home Energy Assistance Program (LI-HEAP)	
<input type="checkbox"/> Workers Compensation	
<input type="checkbox"/> Vocational Rehabilitation Services	



Exhibit E, Attachment B

<input type="checkbox"/> Foster Care (IV-E)	
<input checked="" type="checkbox"/> State Children's Health Insurance Program (CHIP)	BENDEX/SDX/SVES IV, SVES-1 Citizenship
<input type="checkbox"/> Women, Infants and Children (W.I.C.)	
<input checked="" type="checkbox"/> Medicare Savings Programs (MSP)	LIS File
<input checked="" type="checkbox"/> Medicare 1144 (Outreach)	Medicare 1144 Outreach File
<input checked="" type="checkbox"/> Other Federally Funded, State-Administered Programs (List Below)	
Program	SSA Data Exchange System(s)
Medi-Cal Access Program (MCAP)	BENDEX/SDX/SVES IV

(2) The State Agency will use each identified data exchange system only for the purpose of administering the specific program for which access to the data exchange system is provided. SSA data exchange systems are protected by the Privacy Act and Federal law prohibits the use of SSA's data for any purpose other than the purpose of administering the specific program for which such data is disclosed. In particular, the State Agency will:

- a) use the **tax return data** disclosed by SSA only to determine individual eligibility for, or the amount of, assistance under a program listed in 26 U.S.C. § 6103(1)(7) and (8).
- b) use **citizenship status data** disclosed by SSA only to determine entitlement of *new applicants* to: (a) the Medicaid program and CHIP pursuant to the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3; or (b) federally funded, state-administered health or income maintenance programs approved by SSA to receive the *SSA Data Set* through the Centers for Medicare & Medicaid Services' (CMS) Federal Data Services Hub (Hub).

Applicants for Social Security numbers (SSN) report their citizenship data at the time they apply for their SSNs; there is no obligation for an individual to report to SSA a change in his or her immigration status until he or she files a claim for benefits.

C. PROGRAM QUESTIONNAIRE: Prior to signing this IEA, the State Agency will complete and submit to SSA a program questionnaire for each of the federally funded, state-administered programs checked in **Table 1** above. SSA will not disclose any data under this IEA until it has received and approved the completed program questionnaire for each of the programs identified in **Table 1** above.



D. TRANSFER OF DATA: SSA will transmit the data to the State Agency under this IEA using the data transmission method identified in **Table 2** below:

TABLE 2

TRANSFER OF DATA
<p><input type="checkbox"/> Data will be transmitted directly between SSA and the State Agency.</p> <p><input checked="" type="checkbox"/> Data will be transmitted directly between SSA and The California Office of Technology (State Transmission/Transfer Component (“STC”)) by File Transfer Management System (FTMS), a secure mechanism approved by SSA. The STC will serve as the conduit between SSA and the State Agency pursuant to the State STC Agreement.</p> <p><input type="checkbox"/> Data will be transmitted directly between SSA and CMS’ Hub by a secure method of transfer approved by SSA. CMS will transmit the <i>SSA Data Set</i> between SSA and the State Agency pursuant to an agreement between SSA and CMS regarding the use of the Hub.</p> <p><input type="checkbox"/> Data will be transmitted [<i>select one: directly between SSA and the Interstate Connection Network (“ICON”) or through the [name of STC Agency/Vendor] as the conduit between SSA and the Interstate Connection Network (“ICON”)</i>]. ICON is a wide area telecommunications network connecting state agencies that administer the state unemployment insurance laws. When receiving data through ICON, the State Agency will comply with the “Systems Security Requirements for SSA Web Access to SSA Information Through the ICON,” attached as Attachment 3.</p>

E. SECURITY PROCEDURES: The State Agency will comply with limitations on use, treatment, and safeguarding of data under the Privacy Act of 1974 (5 U.S.C. § 552a), as amended by the Computer Matching and Privacy Protection Act of 1988, related Office of Management and Budget guidelines, the Federal Information Security Management Act of 2002 (44 U.S.C. § 3541, et seq.), and related National Institute of Standards and Technology guidelines. In addition, the State Agency will comply with SSA’s “Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration,” attached as **Attachment 4**, as well as the Security Certification Requirements for use of the *SSA Data Set* transmitted via CMS’ Hub, attached as **Attachment 5**. The SSA security controls identified under **Attachment 4** of this IEA prevail for all SSA data received by the State Agency, as identified in Table 1 of this IEA. For any tax return data, the State Agency will also comply with the “Tax Information Security Guidelines for Federal, State and Local Agencies,” Publication 1075, published by the Secretary of the Treasury and available at the following Internal Revenue Service (IRS) website: <http://www.irs.gov/pub/irs-pdf/p1075.pdf>. This IRS Publication 1075 is incorporated by reference into this IEA.

F. STATE AGENCY’S RESPONSIBILITIES: The State Agency will not direct individuals to SSA field offices to obtain data that the State Agency is authorized to receive under this IEA in accordance with Table 1. Where disparities exist between individual-supplied data and SSA’s data, the State Agency will take the following steps before referring the individual to an SSA field office:



- Check its records to be sure that the data of the original submission has not changed (e.g., last name recently changed);
- Contact the individual to verify the data submitted is accurate; and,
- Consult with the SSA Regional Office Contact to discuss options before advising individuals to contact SSA for resolution. The Regional Office Contact will inform the State Agency of the current protocol through which the individual should contact SSA, i.e., visiting the field office, calling the national network service number, or creating an online account via *my* Social Security.

G. CONTRACTOR/AGENT RESPONSIBILITIES: The State Agency will restrict access to the data obtained from SSA to only those authorized State employees, contractors, and agents who need such data to perform their official duties in connection with purposes identified in this IEA. At SSA's request, the State Agency will obtain from each of its contractors and agents a current list of the employees of its contractors and agents who have access to SSA data disclosed under this IEA. The State Agency will require its contractors, agents, and all employees of such contractors or agents with authorized access to the SSA data disclosed under this IEA, to comply with the terms and conditions set forth in this IEA, and not to duplicate, disseminate, or disclose such data without obtaining SSA's prior written approval. In addition, the State Agency will comply with the limitations on use, duplication, and redisclosure of SSA data set forth in Section IX. of the CMPPA Agreement, especially with respect to its contractors and agents.

H. SAFEGUARDING AND REPORTING RESPONSIBILITIES FOR PERSONALLY IDENTIFIABLE INFORMATION ("PII"):

1. The State Agency will ensure that its employees, contractors, and agents:
 - a. properly safeguard PII furnished by SSA under this IEA from loss, theft, or inadvertent disclosure;
 - b. understand that they are responsible for safeguarding this information at all times, regardless of whether or not the State employee, contractor, or agent is at his or her regular duty station;
 - c. ensure that laptops and other electronic devices/media containing PII are encrypted and/or password protected;
 - d. send emails containing PII only if encrypted or if to and from addresses that are secure; and
 - e. limit disclosure of the information and details relating to a PII loss only to those with a need to know.
2. If an employee of the State Agency or an employee of the State Agency's contractor or agent becomes aware of suspected or actual loss of PII, he or she must immediately contact the State Agency official responsible for Systems Security designated below or his or her delegate. That State Agency official or delegate must then notify the SSA Regional Office Contact and the SSA Systems Security Contact identified below. If, for any reason, the responsible State Agency official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within 1 hour, the responsible State Agency official or delegate must report the incident by contacting SSA's National Network Service Center at 1-877-697-4889. The responsible State Agency official or delegate will use the worksheet, attached as **Attachment 6**, to quickly gather and



organize information about the incident. The responsible State Agency official or delegate must provide to SSA timely updates as any additional information about the loss of PII becomes available.

3. SSA will make the necessary contact within SSA to file a formal report in accordance with SSA procedures. SSA will notify the Department of Homeland Security's United States Computer Emergency Readiness Team if loss or potential loss of PII related to a data exchange under this IEA occurs.
4. If the State Agency experiences a loss or breach of data, it will determine whether or not to provide notice to individuals whose data has been lost or breached and bear any costs associated with the notice or any mitigation.

I. POINTS OF CONTACT:

FOR SSA

San Francisco Regional Office:

Nancy Borjon
Data Exchange Coordinator
Frank Hagel Federal Building
1221 Nevin Avenue
Richmond, CA 94801
Phone: (510) 970-8256
Fax: (510) 970-8101
Email: Nancy.Borjon@ssa.gov

Data Exchange Issues:

Sarah Reagan
Government Information Specialist
Office of the General Counsel
Office of Privacy and Disclosure
617 Altmeyer
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-9127
Fax: (410) 594-0115
Email: Sarah.Reagan@ssa.gov

Program and Policy Issues:

Michael Wilkins
State Liaison Program Manager
Office of Retirement and Disability Policy
Office of Data Exchange and Policy
Publications
Office of Data Exchange
3609 Annex Building
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 966-4965
Fax: (410) 966-4054
Email: Michael.Wilkins@ssa.gov

Systems Security Issues:

Sean Hagan, Acting Director
Division of Compliance and
Assessments
Office of Information Security
Office of Systems
Social Security Administration
3829 Annex Building
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-4519
Fax: (410) 597-0845
Email: Sean.Hagan@ssa.gov

Systems Issues:

Michelle J. Anderson, Branch Chief
DBIAE/Data Exchange and Verification
Branch



Office of Information Technology Business
Support

Office of Systems
3-D-1 Robert M. Ball Building
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-5943
Fax: (410) 966-3147
Email: Michelle.J.Anderson@ssa.gov

FOR STATE AGENCY

Agreement Issues:

Rocky Evans
Chief, Eligibility Administration Section
Program Review Branch
Medi-Cal Eligibility Division (MCED)
1501 Capitol Avenue
Sacramento, CA 95814
Phone: (916) 319-8434
Fax: (916) 552-9477
Email: Rocky.Evans@dhcs.ca.gov

Technical Issues:

YK Chalamcherla
Chief, Application Development &
Support Branch
Enterprise Innovative Technology
Services (EITS)
1501 Capitol Avenue
Sacramento, CA 95814
Phone: (916) 322-8044
Fax: (916) 440-7065
Email: YK.Chalamcherla@dhcs.ca.gov

Sean Wieland
Chief, Business & Application
Integration Section
Enterprise Innovative Technology
Services (EITS)
1501 Capitol Avenue
Sacramento, CA 95814
Phone: (916) 550-7088
Fax: (916) 440-7065
Email: Sean.Wieland@dhcs.ca.gov

- J. DURATION:** The effective date of this IEA is March 6, 2017. This IEA will remain in effect for as long as: (1) a CMPPA Agreement governing this IEA is in effect between SSA and the State or the State Agency; and (2) the State Agency submits a certification in accordance with Section K. below at least 30 days before the expiration and renewal of such CMPPA Agreement.
- K. CERTIFICATION AND PROGRAM CHANGES:** At least 30 days before the expiration and renewal of the State CMPPA Agreement governing this IEA, the State Agency will certify in writing to SSA that: (1) it is in compliance with the terms and conditions of this IEA; (2) the data exchange processes under this IEA have been and will be conducted without change; and (3) it will, upon SSA's request, provide audit reports or other documents that demonstrate review and oversight activities. If there are substantive changes in any of the programs or data exchange processes listed in this IEA, the parties will modify the IEA in



accordance with Section L. below and the State Agency will submit for SSA's approval new program questionnaires under Section C. above describing such changes prior to using SSA's data to administer such new or changed program.

L. MODIFICATION: Modifications to this IEA must be in writing and agreed to by the parties.

M. TERMINATION: The parties may terminate this IEA at any time upon mutual written consent. In addition, either party may unilaterally terminate this IEA upon 90 days advance written notice to the other party. Such unilateral termination will be effective 90 days after the date of the notice, or at a later date specified in the notice.

SSA may immediately and unilaterally suspend the data flow under this IEA, or terminate this IEA, if SSA, in its sole discretion, determines that the State Agency (including its employees, contractors, and agents) has: (1) made an unauthorized use or disclosure of SSA-supplied data; or (2) violated or failed to follow the terms and conditions of this IEA or the CMPPA Agreement.

N. INTEGRATION: This IEA, including all attachments, constitutes the entire agreement of the parties with respect to its subject matter. There have been no representations, warranties, or promises made outside of this IEA. This IEA shall take precedence over any other document that may be in conflict with it.

ATTACHMENTS

- 1 – CMPPA Agreement
- 2 – SSA Data Exchange Systems
- 3 – Systems Security Requirements for SSA Web Access to SSA Information Through ICON
- 4 – Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration
- 5 – Security Certification Requirements for use of the *SSA Data Set* Transmitted via CMS' Hub
- 6 – PII Loss Reporting Worksheet



O. AUTHORIZED SIGNATURES: The signatories below warrant and represent that they have competent authority on behalf of their respective agency to enter into the obligations set forth in this IEA.

SOCIAL SECURITY ADMINISTRATION
REGION IX



Grace M. Kim
Regional Commissioner

05/03/2017

Date

THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES



Jennifer Kent
Director, California Department of Health Care Services

4/7/17

Date



**CERTIFICATION OF COMPLIANCE
FOR
THE INFORMATION EXCHANGE AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION (SSA)
AND
THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES (STATE
AGENCY)
(State Agency Level)**

In accordance with the terms of the Information Exchange Agreement (IEA/F) between SSA and the State Agency, the State Agency, through its authorized representative, hereby certifies that, as of the date of this certification:

1. The State Agency is in compliance with the terms and conditions of the IEA/F;
2. The State Agency has conducted the data exchange processes under the IEA/F without change, except as modified in accordance with the IEA/F;
3. The State Agency will continue to conduct the data exchange processes under the IEA/F without change, except as may be modified in accordance with the IEA/F;
4. Upon SSA's request, the State Agency will provide audit reports or other documents that demonstrate compliance with the review and oversight activities required under the IEA/F and the governing Computer Matching and Privacy Protection Act Agreement; and
5. In compliance with the requirements of the "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration," (last updated July 2015) Attachment 4 to the IEA/F, as periodically updated by SSA, the State Agency has not made any changes in the following areas that could potentially affect the security of SSA data:
 - General System Security Design and Operating Environment
 - System Access Control
 - Automated Audit Trail
 - Monitoring and Anomaly Detection
 - Management Oversight
 - Data and Communications Security
 - Contractors of Electronic Information Exchange Partners
 - Cloud Service Providers for Electronic Information Exchange Partners

The State Agency will submit an updated Security Design Plan at least 30 days prior to making any changes to the areas listed above and provide updated contractor employee lists before allowing new employees' access to SSA provided data.

6. The State Agency agrees that use of computer technology to transfer the data is more economical, efficient, and faster than using a manual process. As such, the State Agency will continue to utilize data exchange to obtain data it needs to administer the programs for which it is authorized, under the IEA/F. Further, before directing an individual to an SSA field office to obtain data, the State Agency will verify that the information it submitted to SSA via data exchange is correct, and verify with the individual that the information he/she supplied is accurate. The use of electronic data exchange expedites program administration and limits SSA field office traffic.

The signatory below warrants and represents that he or she is a representative of the State Agency duly authorized to make this certification on behalf of the State Agency.

DEPARTMENT OF HEALTH CARE SERVICES OF CALIFORNIA



Jennifer Kent
Director

5/17/17

Date

ATTACHMENT 1

**COMPUTER MATCHING AND PRIVACY PROTECTION ACT AGREEMENT
(CMPPA)**

COMPUTER MATCHING AND PRIVACY PROTECTION ACT AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION
AND
THE HEALTH AND HUMAN SERVICES AGENCY
OF CALIFORNIA

I. Purpose and Legal Authority

A. Purpose

This Computer Matching and Privacy Protection Act (CMPPA) Agreement (Agreement) between the Social Security Administration (SSA) and the Health and Human Services Agency of California (State Agency) sets forth the terms and conditions governing disclosures of records, information, or data (collectively referred to herein as "data") made by SSA to the State Agency that administers federally funded benefit programs, including those under various provisions of the Social Security Act (Act), such as section 1137 (42 U.S.C. § 1320b-7), as well as the state-funded state supplementary payment programs under Title XVI of the Act. The terms and conditions of this Agreement ensure that SSA makes such disclosures of data, and the State Agency uses such disclosed data, in accordance with the requirements of the Privacy Act of 1974, as amended by the CMPPA of 1988, 5 U.S.C. § 552a.

Under section 1137 of the Act, the State Agency is required to use an income and eligibility verification system to administer specified federally funded benefit programs, including the state-funded state supplementary payment programs under Title XVI of the Act. To assist the State Agency in determining entitlement to and eligibility for benefits under those programs, as well as other federally funded benefit programs, SSA discloses certain data about applicants (and in limited circumstances, members of an applicant's household), for state benefits from SSA Privacy Act Systems of Records (SOR) and verifies the Social Security numbers (SSN) of the applicants.

B. Legal Authority

SSA's authority to disclose data and the State Agency's authority to collect, maintain, and use data protected under SSA SORs for specified purposes is:

- Sections 453, 1106(b), and 1137 of the Act (42 U.S.C. §§ 653, 1306(b), and 1320b-7) (income and eligibility verification data);
- 26 U.S.C. § 6103(1)(7) and (8) (tax return data);
- Section 202(x)(3)(B)(iv) of the Act (42 U.S.C. § 402(x)(3)(B)(iv)) and Section 1611(e)(1)(I)(iii) of the Act (42 U.S.C. § 1382(e)(1)(I)(iii)) (prisoner data);

- Section 205(r)(3) of the Act (42 U.S.C. § 405(r)(3)) and the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, § 7213(a)(2) (death data);
- Sections 402, 412, 421, and 435 of Pub. L. 104-193 (8 U.S.C. §§ 1612, 1622, 1631, and 1645) (quarters of coverage data);
- Children's Health Insurance Program Reauthorization Act of 2009 (CHIPRA), Pub. L. 111-3 (citizenship data); and
- Routine use exception to the Privacy Act, 5 U.S.C. § 552a(b)(3) (data necessary to administer other programs compatible with SSA programs).

This Agreement further carries out section 1106(a) of the Act (42 U.S.C. § 1306), the regulations promulgated pursuant to that section (20 C.F.R. Part 401), the Privacy Act of 1974 (5 U.S.C. § 552a), as amended by the CMPPA, related Office of Management and Budget (OMB) guidelines, the Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. § 3541, et seq.), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); and related National Institute of Standards and Technology (NIST) guidelines, which provide the requirements that the State Agency must follow with regard to use, treatment, and safeguarding of data.

II. Scope

- A. The State Agency will comply with the terms and conditions of this Agreement and the Privacy Act, as amended by the CMPPA.
- B. The State Agency will execute an Information Exchange Agreement (IEA) with SSA, documenting additional terms and conditions applicable to those specific data exchanges, including the particular benefit programs administered by the State Agency, the data elements that will be disclosed, and the data protection requirements implemented to assist the State Agency in the administration of those programs.
- C. The State Agency will use the SSA data governed by this Agreement to determine entitlement and eligibility of individuals for one or more of the following programs, which are specifically identified in the IEA:
 1. Temporary Assistance to Needy Families (TANF) program under Part A of Title IV of the Act;
 2. Medicaid provided under an approved State plan or an approved waiver under Title XIX of the Act;
 3. State Children's Health Insurance Program (CHIP) under Title XXI of the Act, as amended by the Children's Health Insurance Program Reauthorization Act of 2009;

4. Supplemental Nutritional Assistance Program (SNAP) under the Food Stamp Act of 1977 (7 U.S.C. § 2011, et seq.);
 5. Women, Infants and Children Program (WIC) under the Child Nutrition Act of 1966 (42 U.S.C. § 1771, et seq.);
 6. Medicare Savings Programs (MSP) under 42 U.S.C. § 1396a(10)(E);
 7. Unemployment Compensation programs provided under a state law described in section 3304 of the Internal Revenue Code of 1954;
 8. Low Income Heating and Energy Assistance (LIHEAP or home energy grants) program under 42 U.S.C. § 8621;
 9. State-administered supplementary payments of the type described in section 1616(a) of the Act;
 10. Programs under a plan approved under Titles I, X, XIV, or XVI of the Act;
 11. Foster Care and Adoption Assistance under Title IV of the Act;
 12. Child Support Enforcement programs under section 453 of the Act (42 U.S.C. § 653);
 13. Other applicable federally funded programs administered by the State Agency under Titles I, IV, X, XIV, XVI, XVIII, XIX, XX, and XXI of the Act; and
 14. Any other federally funded programs administered by the State Agency that are compatible with SSA's programs.
- D. The State Agency will ensure that SSA data disclosed for the specific purpose of administering a particular federally funded benefit program is used only to administer that program.

III. Justification and Expected Results

A. Justification

This Agreement and related data exchanges with the State Agency are necessary for SSA to assist the State Agency in its administration of federally funded benefit programs by providing the data required to accurately determine entitlement and eligibility of individuals for benefits provided under these programs. SSA uses computer technology to transfer the data because it is more economical, efficient, and faster than using manual processes.

B. Expected Results

The State Agency will use the data provided by SSA to improve public service and program efficiency and integrity. The use of SSA data expedites the application process and ensures that benefits are awarded only to applicants that satisfy the State Agency's program criteria. A cost-benefit analysis for the exchange made under this Agreement is not required in accordance with the determination by the SSA Data Integrity Board (DIB) to waive such analysis pursuant to 5 U.S.C. § 552a(u)(4)(B).

IV. Record Description

A. Systems of Records (SOR)

SSA SORs used for purposes of the subject data exchanges include:

- 60-0058 -- Master Files of SSN Holders and SSN Applications;
- 60-0059 -- Earnings Recording and Self-Employment Income System;
- 60-0090 -- Master Beneficiary Record;
- 60-0103 -- Supplemental Security Income Record (SSR) and Special Veterans Benefits (SVB);
- 60-0269 -- Prisoner Update Processing System (PUPS); and
- 60-0321 -- Medicare Part D and Part D Subsidy File.

The State Agency will only use the tax return data contained in **SOR 60-0059** (Earnings Recording and Self-Employment Income System) in accordance with 26 U.S.C. § 6103.

B. Data Elements

Data elements disclosed in computer matching governed by this Agreement are Personally Identifiable Information (PII) from specified SSA SORs, including names, SSNs, addresses, amounts, and other information related to SSA benefits and earnings information. Specific listings of data elements are available at:

<http://www.ssa.gov/dataexchange/>

C. Number of Records Involved

The maximum number of records involved in this matching activity is the number of records maintained in SSA's SORs listed above in Section IV.A.

V. Notice and Opportunity to Contest Procedures

A. Notice to Applicants

The State Agency will notify all individuals who apply for federally funded, state-administered benefits that any data they provide are subject to verification through computer matching with SSA. The State Agency and SSA will provide such notice through appropriate language printed on application forms or separate handouts.

B. Notice to Beneficiaries/Recipients/Annuitants

The State Agency will provide notice to beneficiaries, recipients, and annuitants under the programs covered by this Agreement informing them of ongoing computer matching with SSA. SSA will provide such notice through publication in the Federal Register and periodic mailings to all beneficiaries, recipients, and annuitants describing SSA's matching activities.

C. Opportunity to Contest

The State Agency will not terminate, suspend, reduce, deny, or take other adverse action against an applicant for or recipient of federally funded, state-administered benefits based on data disclosed by SSA from its SORs until the individual is notified in writing of the potential adverse action and provided an opportunity to contest the planned action. "Adverse action" means any action that results in a termination, suspension, reduction, or final denial of eligibility, payment, or benefit. Such notices will:

1. Inform the individual of the match findings and the opportunity to contest these findings;
2. Give the individual until the expiration of any time period established for the relevant program by a statute or regulation for the individual to respond to the notice. If no such time period is established by a statute or regulation for the program, a 30-day period will be provided. The time period begins on the date on which notice is mailed or otherwise provided to the individual to respond; and
3. Clearly state that, unless the individual responds to the notice in the required time period, the State Agency will conclude that the SSA data are correct and will effectuate the planned action or otherwise make the necessary adjustment to the individual's benefit or entitlement.

VI. Records Accuracy Assessment and Verification Procedures

Pursuant to 5 U.S.C. § 552a(p)(1)(A)(ii), SSA's DIB has determined that the State Agency may use SSA's benefit data without independent verification. SSA has independently assessed the accuracy of its benefits data to be more than 99 percent accurate when the benefit record is created.

Prisoner and death data, some of which is not independently verified by SSA, does not have the same degree of accuracy as SSA's benefit data. Therefore, the State Agency must independently verify these data through applicable State verification procedures and the notice and opportunity to contest procedures specified in Section V of this Agreement before taking any adverse action against any individual.

Based on SSA's Office of Quality Review "Fiscal Year 2014 Enumeration Accuracy Report," the SSA Enumeration System database (the Master Files of SSN Holders and SSN Applications System) used for SSN matching is 99 percent accurate for records updated by SSA employees.

Individuals applying for SSNs report their citizenship status at the time they apply for their SSNs. There is no obligation for an individual to report to SSA a change in his or her immigration status until he or she files for a Social Security benefit. The State Agency must independently verify citizenship data through applicable State verification procedures and the notice and opportunity to contest procedures specified in Section V of this Agreement before taking any adverse action against any individual.

VII. Disposition and Records Retention of Matched Items

- A. The State Agency will retain all data received from SSA to administer programs governed by this Agreement only for the required processing times for the applicable federally funded benefit programs and will then destroy all such data.
- B. The State Agency may retain SSA data in hardcopy to meet evidentiary requirements, provided that they retire such data in accordance with applicable state laws governing the State Agency's retention of records.
- C. The State Agency may use any accretions, deletions, or changes to the SSA data governed by this Agreement to update their master files of federally funded, state-administered benefit program applicants and recipients and retain such master files in accordance with applicable state laws governing the State Agency's retention of records.
- D. The State Agency may not create separate files or records comprised solely of the data provided by SSA to administer programs governed by this Agreement.
- E. SSA will delete electronic data input files received from the State Agency after it processes the applicable match. SSA will retire its data in accordance with the Federal Records Retention Schedule (44 U.S.C. § 3303a).

VIII. Security Procedures

SSA and the State Agency will comply with the security and safeguarding requirements of the Privacy Act, as amended by the CMPPA, related OMB guidelines, FISMA, related NIST guidelines, and the current revision of Internal Revenue Service (IRS) Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*, available at <http://www.irs.gov>. In addition, SSA

and the State Agency will have in place administrative, technical, and physical safeguards for the matched data and results of such matches. Additional administrative, technical, and physical security requirements governing all data SSA provides electronically to the State Agency, including SSA's *Electronic Information Exchange Security Requirements and Procedures for State and local Agencies Exchanging Electronic Information with SSA*, as well as specific guidance on safeguarding and reporting responsibilities for PII, are set forth in the IEAs.

SSA has the right to monitor the State Agency's compliance with FISMA, the terms of this Agreement, and the IEA and to make onsite inspections of the State Agency for purposes of auditing compliance, if necessary, during the lifetime of this Agreement or of any extension of this Agreement. This right includes onsite inspection of any entity that receives SSA information from the State Agency under the terms of this Agreement, if SSA determines it is necessary.

IX. Records Usage, Duplication, and Redisclosure Restrictions

- A. The State Agency will use and access SSA data and the records created using that data only for the purpose of verifying eligibility for the specific federally funded benefit programs identified in the IEA.
- B. The State Agency will comply with the following limitations on use, duplication, and redisclosure of SSA data:
 1. The State Agency will not use or redisclose the data disclosed by SSA for any purpose other than to determine eligibility for, or the amount of, benefits under the state-administered income/health maintenance programs identified in this Agreement.
 2. The State Agency will not extract information concerning individuals who are neither applicants for, nor recipients of, benefits under the state-administered income/health maintenance programs identified in this Agreement. In limited circumstances that are approved by SSA, the State Agency may extract information about an individual other than the applicant/recipient when the applicant/recipient has provided identifying information about the individual and the individual's income or resources affect the applicant's/recipient's eligibility for such program.
 3. The State Agency will not disclose to an applicant/recipient information about another individual (i.e., an applicant's household member) without the written consent from the individual to whom the information pertains.
 4. The State Agency will use the Federal tax information (FTI) disclosed by SSA only to determine individual eligibility for, or the amount of, assistance under a state plan pursuant to section 1137 programs and child support enforcement

programs in accordance with 26 U.S.C. § 6103(l)(7), and (8). The State Agency receiving FTI will maintain all FTI from IRS in accordance with 26 U.S.C. § 6103(p)(4) and the IRS Publication 1075. Contractors and agents acting on behalf of the State Agency will only have access to tax return data where specifically authorized by 26 U.S.C. § 6103 and the current revision IRS Publication 1075.

5. The State Agency will use the citizenship status data disclosed by SSA only to determine entitlement of new applicants to: (a) the Medicaid program and CHIP pursuant to CHIPRA, Pub. L. 111-3; or (b) federally funded, state-administered health or income maintenance programs approved by SSA. The State Agency will further comply with additional terms and conditions regarding use of citizenship data, as set forth in the State Agency's IEA.
6. The State Agency will restrict access to the data disclosed by SSA to only those authorized State employees, contractors, and agents who need such data to perform their official duties in connection with the purposes identified in this Agreement.
7. The State Agency will enter into a written agreement with each of its contractors and agents who need SSA data to perform their official duties whereby such contractor or agent agrees to abide by all relevant Federal laws, restrictions on access, use, and disclosure, and security requirements in this Agreement. The State Agency will provide its contractors and agents with copies of this Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing this Agreement, and thereafter at SSA's request, the State Agency will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to SSA data and provide such lists to SSA.
8. If the State Agency is authorized or required – pursuant to an applicable law, regulation, or intra-governmental documentation – to provide SSA data to another State or local government entity for the administration of the federally funded, state-administered programs covered by this Agreement, the State Agency must ensure that the State or local government entity, including its employees, abides by all relevant Federal laws, restrictions on access, use, and disclosure, and security requirements in this Agreement and the IEA. At SSA's request, the State Agency will provide copies of any applicable law, regulation, or intra-governmental documentation that authorizes the intra-governmental relationship with the State or local government entity. Upon request from SSA, the State Agency will also establish how it ensures that State or local government entity complies with the terms of this Agreement and the IEA.
9. The State Agency's employees, contractors, and agents who access, use, or disclose SSA data in a manner or purpose not authorized by this Agreement

may be subject to civil and criminal sanctions pursuant to applicable Federal statutes.

10. The State Agency will conduct triennial compliance reviews of its contractor(s) and agent(s) no later than three years after the initial approval of the security certification to SSA. The State Agency will share documentation of its recurring compliance reviews with its contractor(s) and agent(s) with SSA. The State Agency will provide documentation to SSA during its scheduled compliance and certification reviews or upon request.
- C. The State Agency will not duplicate in a separate file or disseminate, without prior written permission from SSA, the data governed by this Agreement for any purpose other than to determine entitlement to, or eligibility for, federally funded benefits. The State Agency proposing the redisclosure must specify in writing to SSA what data are being disclosed, to whom, and the reasons that justify the redisclosure. SSA will not give permission for such redisclosure unless the redisclosure is required by law or essential to the conduct of the matching program and authorized under a routine use. To the extent SSA approves the requested redisclosure, the State Agency will ensure that any entity receiving the redisclosed data will comply with the procedures and limitations on use, duplication, and redisclosure of SSA data, as well as all administrative, technical, and physical security requirements governing all data SSA provides electronically to the State Agency including specific guidance on safeguarding and reporting responsibilities for PII, as set forth in this Agreement and the accompanying IEAs.

X. Comptroller General Access

The Comptroller General (the Government Accountability Office) may have access to all records of the State Agency that the Comptroller General deems necessary to monitor and verify compliance with this Agreement in accordance with 5 U.S.C. § 552a(o)(1)(K).

XI. Duration, Modification, and Termination of the Agreement

A. Duration

1. This Agreement is effective from July 1, 2017 (Effective Date) through December 31, 2018 (Expiration Date).
2. In accordance with the CMPPA, SSA will: (a) publish a Computer Matching Notice in the Federal Register at least 30 days prior to the Effective Date; (b) send required notices to the Congressional committees of jurisdiction under 5 U.S.C. § 552a(o)(2)(A)(i) at least 40 days prior to the

Effective Date; and (c) send the required report to OMB at least 40 days prior to the Effective Date.

3. Within 3 months prior the Expiration Date, the SSA DIB may, without additional review, renew this Agreement for a period not to exceed 12 months, pursuant to 5 U.S.C. § 552a(o)(2)(D), if:
 - the applicable data exchange will continue without any change; and
 - SSA and the State Agency certify to the DIB in writing that the applicable data exchange has been conducted in compliance with this Agreement.
4. If either SSA or the State Agency does not wish to renew this Agreement, it must notify the other party of its intent not to renew at least 3 months prior to the Expiration Date.

B. Modification

Any modification to this Agreement must be in writing, signed by both parties, and approved by the SSA DIB.

C. Termination

The parties may terminate this Agreement at any time upon mutual written consent of both parties. Either party may unilaterally terminate this Agreement upon 90 days advance written notice to the other party; such unilateral termination will be effective 90 days after the date of the notice, or at a later date specified in the notice.

SSA may immediately and unilaterally suspend the data flow or terminate this Agreement if SSA determines, in its sole discretion, that the State Agency has violated or failed to comply with this Agreement.

XII. Reimbursement

In accordance with section 1106(b) of the Act, the Commissioner of SSA has determined not to charge the State Agency the costs of furnishing the electronic data from the SSA SORs under this Agreement.

XIII. Disclaimer

SSA is not liable for any damages or loss resulting from errors in the data provided to the State Agency under any IEAs governed by this Agreement. Furthermore, SSA

is not liable for any damages or loss resulting from the destruction of any materials or data provided by the State Agency.

The performance or delivery by SSA of the goods and/or services described herein and the timeliness of said delivery are authorized only to the extent that they are consistent with proper performance of the official duties and obligations of SSA and the relative importance of this request to others. If for any reason SSA delays or fails to provide services, or discontinues the services or any part thereof, SSA is not liable for any damages or loss resulting from such delay or for any such failure or discontinuance.

XIV. Points of Contact

A. SSA Point of Contact

San Francisco Regional Office:

Jamie Lucero, Director

San Francisco Regional Office, Center for Disability and Programs Support

1221 Nevin Ave., 6th Floor

Richmond, CA 94801

Phone: 510-970-8297

Fax: 510-970-8101

Email: Jamie.Lucero@ssa.gov

B. State Agency Point of Contact

Sonia Herrera

California Health and Human Services Agency

1600 Ninth Street

Sacramento, CA 95814

Phone: 916-654-3459 / Fax: 916-440-5001

Email: Sonia.Herrera@chhs.ca.gov

XV. SSA and Data Integrity Board Approval of Model CMPPA Agreement

The signatories below warrant and represent that they have the competent authority on behalf of SSA to approve the model of this CMPPA Agreement.

SOCIAL SECURITY ADMINISTRATION



Mary Ann Zimmerman
Acting Deputy Executive Director
Office of Privacy and Disclosure
Office of the General Counsel


Date

I certify that the SSA Data Integrity Board approved the model of this CMPPA Agreement.



Glenn Sklar
Acting Chair
SSA Data Integrity Board


Date

XVI. Authorized Signatures

The signatories below warrant and represent that they have the competent authority on behalf of their respective agency to enter into the obligations set forth in this Agreement.

SOCIAL SECURITY ADMINISTRATION

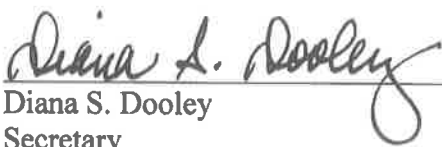


Grace M. Kim
Regional Commissioner
San Francisco

6/2/17

Date

HEALTH AND HUMAN SERVICES AGENCY



Diana S. Dooley
Secretary

May 24, 2017

Date

ATTACHMENT 2

AUTHORIZED DATA EXCHANGE SYSTEM(S)

Authorized Data Exchange System(s)

BEER (Beneficiary Earnings Exchange Record): Employer data for the last calendar year.

BENDEX (Beneficiary and Earnings Data Exchange): Primary source for Title II eligibility, benefit and demographic data.

LIS (Low-Income Subsidy): Data from the Low-Income Subsidy Application for Medicare Part D beneficiaries -- used for Medicare Savings Programs (MSP).

Medicare 1144 (Outreach): Lists of individuals on SSA roles, who may be eligible for medical assistance for: payment of the cost of Medicare cost-sharing under the Medicaid program pursuant to Sections 1902(a)(10)(E) and 1933 of the Act; transitional assistance under Section 1860D-31(f) of the Act; or premiums and cost-sharing subsidies for low-income individuals under Section 1860D-14 of the Act.

PUPS (Prisoner Update Processing System): Confinement data received from over 2000 state and local institutions (such as jails, prisons, or other penal institutions or correctional facilities) -- PUPS matches the received data with the MBR and SSR benefit data and generates alerts for review/action.

QUARTERS OF COVERAGE (QC): Quarters of Coverage data as assigned and described under Title II of the Act -- The term "quarters of coverage" is also referred to as "credits" or "Social Security credits" in various SSA public information documents, as well as to refer to "qualifying quarters" to determine entitlement to receive Food Stamps.

SDX (SSI State Data Exchange): Primary source of Title XVI eligibility, benefit and demographic data as well as data for Title VIII Special Veterans Benefits (SVB).

SOLQ/SOLQ-I (State On-line Query/State On-line Query-Internet): A real-time online system that provides SSN verification and MBR and SSR benefit data similar to data provided through SVES.

Attachment 2

SVES (State Verification and Exchange System): A batch system that provides SSN verification, MBR benefit information, and SSR information through a uniform data response based on authorized user-initiated queries. The SVES types are divided into five different responses as follows:

- | | |
|----------------------------|---|
| SVES I: | This batch provides strictly SSN verification. |
| SVES I/Citizenship* | This batch provides strictly SSN verification and citizenship data. |
| SVES II: | This batch provides strictly SSN verification and MBR benefit information |
| SVES III: | This batch provides strictly SSN verification and SSR/SVB. |
| SVES IV: | This batch provides SSN verification, MBR benefit information, and SSR/SVB information, which represents all available SVES data. |

** Citizenship status data disclosed by SSA under the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3 is only for the purpose of determining entitlement to Medicaid and CHIP program for new applicants.*



ATTACHMENT 3

SYSTEM SECURITY REQUIREMENTS THROUGH THE ICON SYSTEM

Not Applicable

Attachment 3

**Systems Security Requirements for SWA Access
to SSA Information Through the ICON System**

12/9/2016

**Systems Security Requirements for SWA Access to
SSA Information Through the ICON System**

A. General Systems Security Standards

SWA's that request and receive information from SSA through the ICON system must comply with the following general systems security standards concerning access to and control of SSA information. The SWA must restrict access to the information to authorized employees who need it to perform their official duties. Similar to IRS requirements, information retrieved from SSA must be stored in a manner that is physically and electronically secure from access by unauthorized persons during both duty and non-duty hours, or when not in use. SSA information must be processed under the immediate supervision and control of authorized personnel. The SWA must employ both physical and electronic safeguards to ensure that unauthorized personnel cannot retrieve SSA information by means of computer, remote terminal or other means.

All persons who will have access to any SSA information must be advised of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and State laws. SSA may, at its discretion, make on-site inspections or other provisions to ensure that adequate safeguards are being maintained by the SWA.

B. System Security Requirements for SWA's

SWA's that receive SSA information through the ICON system must comply with the following systems security requirements which must be met before DOL will approve a request from an SWA for online access to SSA information through the ICON system. The SWA system security design and procedures must conform to these requirements. They must be documented by the SWA and subsequently certified by either DOL or by an Independent Verification and Validation (IV&V) contractor prior to initiating transactions to and from SSA through the ICON.

No specific format for submitting this documentation to DOL is required. However, regardless of how it is presented, the information should be submitted to DOL in both hardcopy and electronic format, and the hardcopy should be submitted over the signature of an official representative of the SWA. Written documentation should address each of the following security control areas:

1. General System Security Design and Operating Environment

The SWA must provide a written description of its' system configuration and security features. This should include the following:

- a. A general description of the major hardware, software and communications platforms currently in use, including a description of the system's security design features and user access controls; and
- b. A description of how SSA information will be obtained by and presented to SWA users, including sample computer screen presentation formats and an explanation of whether the SWA system will request information from SSA by means of systems generated or user initiated transactions; and
- c. A description of the organizational structure and relationships between systems managers, systems security personnel, and users, including an estimate of the number of users that will have access to SSA data within the SWA system and an explanation of their job descriptions.

Meeting this Requirement

SWA's must explain in their documentation the overall design and security features of their system. During onsite certification, the IV&V contractor, or other certifier, will use the SWA's design documentation and discussion of the additional systems security requirements (following) as their guide for conducting the onsite certification and for verifying that the SWA systems and procedures conform to SSA requirements.

Following submission to the DOL in connection with the initial certification process, the documentation must be updated any time significant architectural changes are made to the system or to its' security features. During its future compliance reviews (see below), the SSA will ask to review the updated design documentation as needed.

2. Automated Audit Trail

SWA's receiving SSA information through the ICON system must implement and maintain a fully automated audit trail system capable of data collection, data retrieval and data storage. At a minimum, data collected through the audit trail system must associate each query transaction to its initiator and relevant business purpose (i.e. the SWA client record for which SSA data was requested), and each transaction must be time and date stamped. Each query transaction must be stored

in the audit file as a separate record, not overlaid by subsequent query transactions.

Access to the audit file must be restricted to authorized users with a “need to know” and audit file data must be unalterable (read only) and maintained for a minimum of three (preferably seven) years. Retrieval of information from the automated audit trail may be accomplished online or through batch access. This requirement must be met before DOL will approve the SWA’s request for access to SSA information through the ICON system.

If SSA-supplied information is retained in the SWA system, or if certain data elements within the SWA system will indicate to users that the information has been verified by SSA, the SWA system also must capture an audit trail record of any user who views SSA information stored within the SWA system. The audit trail requirements for these inquiry transactions are the same as those outlined above for SWA transactions requesting information directly from SSA.

Meeting this Requirement

The SWA must include in their documentation a description of their audit trail capability and a discussion of how it conforms to SSA’s requirements. During onsite certification, the IV&V contractor, or other certifier, will request a demonstration of the system’s audit trail and retrieval capability. The SWA must be able to identify employee’s who initiate online requests for SSA information (or, for systems generated transaction designs, the SWA case that triggered the transaction), the time and date of the request, and the purpose for which the transaction was originated. The certifier, or IV&V contractor, also will request a demonstration of the system’s audit trail capability for tracking the activity of SWA employees that are permitted to view SSA supplied information within the SWA system, if applicable.

During its future compliance reviews (see below), the SSA also will test the SWA audit trail capability by requesting verification of a sample of transactions it has processed from the SWA after implementation of access to SSA information through the ICON system.

3. System Access Control

The SWA must utilize and maintain technological (logical) access controls that limit access to SSA information to only those users authorized for such access based on their official duties. The SWA must use a recognized user access security software package (e.g. RAC-F, ACF-2, TOP SECRET) or an equivalent security software design. The access control software must utilize personal identification numbers (PIN) and passwords (or biometric identifiers) in combination with the user’s system identification code. The SWA must have

management control and oversight of the function of authorizing individual user access to SSA information, and over the process of issuing and maintaining access control PINs and passwords for access to the SWA system.

Meeting this Requirement

The SWA must include in their documentation a description of their technological access controls, including identifying the type of software used, an overview of the process used to grant access to protected information for workers in different job categories, and a description of the function responsible for PIN/password issuance and maintenance.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individual(s) responsible for these functions to verify their responsibilities in the SWA's access control process and will observe a demonstration of the procedures for logging onto the SWA system and for accessing SSA information.

4. Monitoring and Anomaly Detection

The SWA's system must include the capability to prevent employees from browsing (i.e. unauthorized access or use of SSA information) SSA records for information not related to an SWA client case (e.g. celebrities, SWA employees, relatives, etc.) If the SWA system design is transaction driven (i.e. employees cannot initiate transactions themselves, rather, the SWA system triggers the transaction to SSA), or if the design includes a "permission module" (i.e. the transaction requesting information from SSA cannot be triggered by an SWA employee unless the SWA system contains a record containing the client's Social Security Number), then the SWA needs only minimal additional monitoring and anomaly detection. If such designs are used, the SWA only needs to monitor any attempts by their employees to obtain information from SSA for clients not in their client system, or attempts to gain access to SSA data within the SWA system by employees not authorized to have access to such information.

If the SWA design does not include either of the security control features described above, then the SWA must develop and implement compensating security controls to prevent their employees from browsing SSA records. These controls must include monitoring and anomaly detection features, either systematic, manual, or a combination thereof. Such features must include the capability to detect anomalies in the volume and/or type of queries requested by individual SWA employees, and systematic or manual procedures for verifying that requests for SSA information are in compliance with valid official business purposes. The SWA system must produce reports providing SWA management and/or supervisors with the capability to appropriately monitor user activity, such as:

- User ID exception reports

This type of report captures information about users who enter incorrect user ID's when attempting to gain access to the system or to the transaction that initiates requests for information from SSA, including failed attempts to enter a password.

- Inquiry match exception reports

This type of report captures information about users who may be initiating transactions for Social Security Numbers that have no client case association within the SWA system.

- System error exception reports

This type of report captures information about users who may not understand or be following proper procedures for access to SSA information through the ICON system.

- Inquiry activity statistical reports

This type of report captures information about transaction usage patterns among authorized users, which would provide SWA management a tool for monitoring typical usage patterns compared to extraordinary usage.

The SWA must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors, or to local security officers, to ensure that the reports are used by those whose responsibilities include monitoring the work of the authorized users.

Meeting this Requirement

The SWA must explain in their documentation how their system design will monitor and/or prevent their employees from browsing SSA information. If the design is based on a "permission module" (see above), a similar design, or is transaction driven (i.e. no employee initiated transactions) then the SWA does not need to implement additional systematic and/or managerial oversight procedures to monitor their employees access to SSA information. The SWA only needs to monitor user access control violations. The documentation should clearly explain how the system design will prevent SWA employees from browsing SSA records.

If the SWA system design permits employee initiated transactions that are uncontrolled (i.e. no systematically enforced relationship to an SWA client), then the SWA must develop and document the monitoring and anomaly detection process they will employ to deter their employees from browsing SSA

information. The SWA should include sample report formats demonstrating their capability to produce the types of reports described above, and the SWA should include a description of the process that will be used to distribute these reports to managers/supervisors, and the management controls that will ensure the reports are used for their intended purpose.

During onsite certification, the IV&V contractor, or other certifier, will request a demonstration of the SWA's monitoring and anomaly detection capability.

- If the design is based on a permission module or similar design, or is transaction driven, the SWA will demonstrate how the system triggers requests for information from SSA.
- If the design is based on a permission module, the SWA will demonstrate the process by which requests for SSA information are prevented for Social Security Numbers not present in the SWA system (e.g. by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the SWA system.)
- If the design is based on systematic and/or managerial monitoring and oversight, the SWA will provide copies of anomaly detection reports and demonstrate the report production capability.

During onsite certification, the IV&V contractor, or other certifier, also will meet with a sample of managers and/or supervisors responsible for monitoring ongoing compliance to assess their level of training to monitor their employee's use of SSA information, and for reviewing reports and taking necessary action.

5. Management Oversight and Quality Assurance

The SWA must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to SSA information through the ICON system, and to ensure there is ongoing compliance with the terms of the SWA's data exchange agreement with SSA. The management oversight function must consist of one or more SWA management officials whose job functions include responsibility for assuring that access to and use of SSA information is appropriate for each employee position type for which access is granted.

This function also should include responsibility for assuring that employees granted access to SSA information receive adequate training on the sensitivity of the information, safeguards that must be followed, and the penalties for misuse, and should perform periodic self-reviews to monitor ongoing usage of the online access to SSA information. In addition, there should be the capability to randomly sample work activity involving online requests for SSA information to

determine whether the requests comply with these guidelines. These functions should be performed by SWA employees whose job functions are separate from those who request or use information from SSA.

Meeting this Requirement

The SWA must document that they will establish and/or maintain ongoing management oversight and quality assurance capabilities for monitoring the issuance and maintenance of user ID's for online access to SSA information, and oversight and monitoring of the use of SSA information within the SWA business process. The outside entity should describe how these functions will be performed within their organization and identify the individual(s) or component(s) responsible for performing these functions.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individual(s) responsible for these functions and request a description of how these responsibilities will be carried out.

6. Security Awareness and Employee Sanctions

The SWA must establish and/or maintain an ongoing function that is responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse. Security awareness training should occur periodically or as needed, and should address the Privacy Act and other Federal and State laws governing use and misuse of protected information. In addition, there should be in place a series of administrative procedures for sanctioning employees who violate these laws through the unlawful disclosure of protected information.

Meeting this Requirement

The SWA must document that they will establish and/or maintain an ongoing function responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse of SSA information. The SWA should describe how these functions will be performed within their organization, identify the individual(s) or component(s) responsible for performing the functions, and submit copies of existing procedures, training material and employee acknowledgment statements.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individuals responsible for these functions and request a description of how these responsibilities are carried out. The IV&V contractor, or other certifier, also will meet with a sample of SWA employees to assess their level of training and

understanding of the requirements and potential sanctions applicable to the use and misuse of SSA information.

7. Data and Communications Security

The encryption method employed must meet acceptable standards designated by the National Institute of Standards and Technology (NIST). The recommended encryption method to secure data in transport for use by SSA is the Advanced Encryption Standard (AES) or triple DES (DES3) if AES is unavailable.

D. Onsite Systems Security Certification Review

The SWA must obtain and participate in an onsite review and compliance certification of their security infrastructure and implementation of these security requirements prior to being permitted to submit online transaction to SSA through the ICON system. DOL will require an initial onsite systems security certification review to be performed by either an independent IV&V contractor, or other DOL approved certifier. The onsite certification will address each of the requirements described above and will include, where appropriate, a demonstration of the SWA's implementation of each requirement. The review will include a walkthrough of the SWA's data center to observe and document physical security safeguards, a demonstration of the SWA's implementation of online access to SSA information through the ICON system, and discussions with managers/supervisors. The IV&V contractor, or other certifier, also will visit at least one of the SWA's field offices to discuss the online access to SSA information with a sample of line workers and managers to assess their level of training and understanding of the proper use and protection of SSA information.

The IV&V contractor, or other certifier, will separately document and certify SWA compliance with each SSA security requirement. To fully comply with SSA's security requirements and be certified to connect to SSA through the ICON system, the SWA must submit to DOL a complete package of documentation as described above and a complete certification from an independent IV&V contractor, or other DOL approved certifier, that the SWA system design and infrastructure is in agreement with the SWA documentation and consistent with SSA requirements. Any unresolved or unimplemented security control features must be resolved by the SWA before DOL will authorize their connection to SSA through the ICON system.

Following initial certification and authorization from DOL to connect to SSA through the ICON system, SSA is responsible for future systems security compliance reviews. SSA conducts such reviews approximately once every three years, or as needed if there is a significant change in the SWA's computing platform, or if there is a violation of any of SSA's systems security requirements or an unauthorized disclosure of SSA information by the SWA. The format of those reviews generally consists of

reviewing and updating the SWA compliance with the systems security requirements described above.

Exhibit E, Attachment B

SENSITIVE DOCUMENT

ATTACHMENT 4

**ELECTRONIC INFORMATION EXCHANGE SECURITY REQUIREMENTS
AND PROCEDURES**

(Technical Systems Security Requirements- TSSR)



**ELECTRONIC INFORMATION EXCHANGE SECURITY
REQUIREMENTS AND PROCEDURES
FOR
STATE AND LOCAL AGENCIES EXCHANGING ELECTRONIC
INFORMATION WITH THE SOCIAL SECURITY
ADMINISTRATION**

SENSITIVE DOCUMENT

**Version 7.0
July 2015**

TABLE OF CONTENTS

1. Introduction
2. Electronic Information Exchange (EIE) Definition
3. Roles and Responsibilities
4. General Systems Security Standards
5. Systems Security Requirements
 - 5.1 Overview
 - 5.2 General System Security Design and Operating Environment
 - 5.3 System Access Control
 - 5.4 Automated Audit Trail
 - 5.5 Personally Identifiable Information (PII)
 - 5.6 Monitoring and Anomaly Detection
 - 5.7 Management Oversight and Quality Assurance
 - 5.8 Data and Communications Security
 - 5.9 Incident Reporting
 - 5.10 Security Awareness and Employee Sanctions
 - 5.11 Contractors of Electronic Information Exchange Partners
 - 5.12 Cloud Service Providers (CSP) for Electronic Information Exchange Partners
6. Security Certification and Compliance Review Programs
 - 6.1 The Security Certification Program
 - 6.2 Documenting Security Controls in the Security Design Plan (SDP)
 - 6.2.1 When the SDP is Required
 - 6.3 The Certification Process
 - 6.4 The Compliance Review Program and Process
 - 6.5.1 EIEP Compliance Review Participation
 - 6.6 Scheduling the Onsite Review
7. Additional Definitions
8. Regulatory References
9. Frequently Asked Questions

1. Introduction

Federal standards require the Social Security Administration (SSA) to maintain oversight of the information it provides to its *Electronic Information Exchange Partners (EIEPs)*. EIEPs must protect the information with efficient and effective security controls. EIEPs are entities that have electronic information exchange agreements with the agency.

This document consistently references the concept of **Electronic Information Exchange Partners (EIEP)**; however, our **Compliance Review Questionnaire (CRQ)** and **Security Design Plan (SDP)** documents will use the terms “state agency” or “state agency, contractor(s), and agent(s)” for clarity. Most state officials and agreement signatories are not familiar with the acronym EIEP; therefore, SSA will continue to use the terms “state agency” or “state agency, contractor(s), and agent(s)” in the same manner as the Computer Matching and Privacy Protection Act (CMPPA) and Information Exchange Agreements (IEA). This allows for easier alignment and mapping back to our data exchange agreements between state agencies and SSA. It will also provide a more “user-friendly” experience for the state officials who complete these forms on behalf of their state agencies.

The objective of this document is twofold. The first is to ensure that SSA can properly certify EIEPs as compliant with SSA security standards, requirements, and procedures. The second is to ensure that EIEPs adequately safeguard electronic information provided to them by SSA.

This document helps EIEPs understand the criteria that SSA uses when evaluating and certifying the system design and security features used for electronic access to SSA-provided information. Finally, this document provides the framework and general procedures for SSA’s Security Certification and Compliance Review Programs.

The primary statutory authority that supports the information contained in this document is the **Federal Information Security Management Act (FISMA)**. FISMA became law as part of the **Electronic Government Act of 2002**. FISMA is the United States legislation that defines a comprehensive framework to protect government information, operations, and assets against natural or manufactured threats. FISMA assigned the **National Institute of Standards and Technology (NIST)**, a branch of the U.S. Department of Commerce, the responsibility to outline and define compliance with FISMA. Unless otherwise stated, all of SSA’s requirements mirror the NIST-defined management, operational, and technical controls listed in the various NIST Special Publications (SP) libraries of technical guidance documents.

To gain electronic access to SSA-provided information, under the auspices of a data exchange agreement, EIEP’s must comply with SSA’s most current **Technical System Security Requirements** (hereafter referred to as **TSSRs**) to gain access to SSA-provided information. This document is **synonymous** with the **Electronic Information Exchange Security Requirements and Procedures for State and**

Local Agencies Exchanging Electronic Information with the Social Security Administration in the agreements. The TSSR specifies minimally acceptable levels of security standards and controls to protect SSA-provided information. SSA maintains the TSSR as a living document—subject to change--that addresses emerging threats, new attack methods and the development of new technology that potentially places SSA-provided information at risk. EIEPs may proactively ensure their ongoing compliance to the TSSR by periodically requesting the most current version from SSA. SSA will work with EIEPs to resolve deficiencies, which result from updates to the TSSRs. SSA refers to this process as **Gap Analysis**. EIEPs may proactively ensure their ongoing compliance with the TSSRs by periodically requesting the most current TSSR package from their SSA Point of Contact (POC) from the data exchange agreement.

SSA's standard for categorization of information (Moderate) and information systems is to provide appropriate levels of security according to risk level. Additions, deletions, or modification of security controls directly affect the level of security and due diligence SSA requires EIEPs use to mitigate risks. The emergence of new threats, attack methods, and the development of new technology warrants frequent reviews and revisions to our TSSR. Consequently, EIEPs should expect SSA's TSSR to evolve in harmony with the industry.

2. Electronic Information Exchange (EIE) Definition

For discussion purposes herein, EIE is any electronic process in which SSA discloses information under its control to any third party for program or non-program purposes, without the specific consent of the subject individual or any agent acting on his or her behalf. EIE involves individual data transactions and data files processed within the programmatic systems of parties to electronic information sharing agreements with SSA. This includes direct terminal access (DTA) to SSA systems, batch processing, and variations thereof (e.g., online query) regardless of the systematic method used to accomplish the activity or to interconnect SSA with the EIEP.

3. Roles and Responsibilities

The SSA *Office of Information Security (OIS)* has agency-wide responsibility for interpreting, developing, and implementing security policy; providing security and integrity review requirements for all major SSA systems; managing SSA's fraud monitoring and reporting activities, developing and disseminating security training and awareness materials, and providing consultation and support for a variety of agency initiatives. SSA's security reviews ensure that external systems receiving information from SSA are secure and operate in a manner consistent with SSA's Information Technology (IT) security policies and in compliance with the terms of electronic data exchange agreements executed by SSA with outside entities. Within the context of SSA's security policies and the terms of the electronic data exchange

agreements with SSA's EIEPs, SSA exclusively conducts and brings to closure initial security certifications and triennial security compliance reviews. This includes (but not limited to) any EIEP that processes, maintains, transmits, or stores SSA-provided information in accordance with pertinent Federal requirements.

- a. The SSA Regional *Data Exchange Coordinators* (DECs) serve as a bridge between SSA and EIEPs. DECs assist in coordinating data exchange security review activities with EIEPs; (e.g., providing points of contact with state agencies, assisting in setting up security reviews, etc.) DECs are also the first points of contact for states if an employee of a state agency or an employee of a state agency's contractor or agent becomes aware of suspected or actual loss of SSA-provided information.
- b. SSA requires **EIEPs** to adhere to the standards, requirements, and procedures, published in this TSSR document.
 - “Personally Identifiable Information (PII),” covered under several Federal laws and statutes, refers to specific information about an individual used to trace that individual's identity. Information such as his/her name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records, alone, or when combined with other personal or identifying information is linkable or lined to a specific individual's medical, educational, financial, and employment information.
 - The data (last 4 digits of the SSN) that SSA provides to its EIEPs for purposes of the Help America Vote Act (HAVA) does not identify a specific individual; therefore, is not “PII” as defined by the Act.
 - Both SSA and EIEPs must remain diligent in the responsibility for establishing *appropriate* management, operational, and technical safeguards to ensure the confidentiality, integrity, and availability of its records and to protect against any anticipated threats or hazards to their security or integrity.
- c. A State Transmission/Transfer Component (STC) is an organization that performs as an electronic information conduit or collection point for one of more other entities (also referred to as a hub). An STC must also adhere to the same management, operational and technical controls as SSA and the EIEP.

NOTE: Disclosure of Federal Tax Information (FTI) is limited to certain Federal agencies and state programs supported by federal statutes under Sections 1137, 453, and 1106 of the Social Security Act. For information regarding

safeguards for protecting FTI, consult IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies.

4. General Systems Security Standards

EIEPs that request and receive information electronically from SSA must comply with the following general systems security standards concerning access to and control of SSA-provided information.

NOTE: EIEPs may not create separate files or records comprised solely of the information provided by SSA.

1. EIEPs must ensure that means, methods, and technology used to process, maintain, transmit, or store SSA-provided information neither prevents nor impedes the EIEP's ability to:
 - safeguard the information in conformance with SSA requirements
 - efficiently investigate fraud, data breaches, or security events that involve SSA-provided information
 - detect instances of misuse or abuse of SSA-provided information

For example, Utilization of cloud computing may have the potential to jeopardize an EIEP's compliance with the terms of their agreement or associated systems security requirements and procedures.

2. The EIEP must use the electronic connection established between the EIEP and SSA only in support of the current agreement(s) between the EIEP and SSA.
3. The EIEP must use the software and/or devices provided to the EIEPs only in support of the current agreement(s) between the EIEPs and SSA.
4. SSA prohibits the EIEP from modifying any software or devices provided to the EIEPs by SSA.
5. EIEPs must ensure that SSA-provided information is not processed, maintained, transmitted, or stored in or by means of data communications channels, electronic devices, computers, or computer networks located in geographic or virtual areas not subject to U.S. law.
6. EIEPs must restrict access to the information to authorized users who need it to perform their official duties.

NOTE: Contractors and agents (hereafter referred to as contractors) of the EIEP who process, maintain, transmit, or store SSA-provided information are held to the same security requirements as employees of the EIEP. Refer to the section '[Contractors of Electronic Information Exchange Partners in the Systems Security Requirements](#)' for additional information.

7. EIEPs must store information received from SSA in a manner that, at all times, is

physically and electronically secure from access by unauthorized persons.

8. The EIEP must process SSA-provided information under the immediate supervision and control of authorized personnel.
9. EIEPs must employ both physical and technological barriers to prevent unauthorized retrieval of SSA-provided information via computer, remote terminal, or other means.
10. EIEPs must have formal PII incident response procedures. When faced with a security incident, caused by malware, unauthorized access, software issues, or acts of nature, the EIEP must be able to respond in a manner that protects SSA-provided information affected by the incident.
11. EIEPs must have an active and robust security awareness program, which is mandatory for all employees who access SSA-provided information.
12. EIEPs must advise employees with access to SSA-provided information of the confidential nature of the information, the safeguards required to protecting the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and state laws.
13. In accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) on Contingency Planning requirements and recommendations, SSA requires EIEPs to document a senior management approved Contingency plan that includes a disaster recovery plan that addresses both natural disaster and cyber-attack situations.
14. SSA requires the Contingency Plan to include details regarding the organizational business continuity plan (BCP) and a business impact analyses (BIA) that address the security of SSA-provided information if a disaster occurs.
15. At its discretion, SSA or its designee must have the option to conduct onsite security reviews or make other provisions, to ensure that EIEPs maintain adequate security controls to safeguard the information we provide.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5. Systems Security Requirements

5.1 Overview

SSA's TSSR represent the current industry standard for security controls, safeguards, and countermeasures required for Federal information systems by Federal regulations, statutes, standards, and guidelines. Additionally, SSA's TSSR includes organizationally defined interpretations, policies, and procedures mandated by the authority of the Commissioner of Social Security in areas when or where other cited authorities may be silent or non-specific.

SSA must certify that the EIEP has implemented security controls that meet the requirements and work as intended, before the authorization to initiate transactions to and from SSA, through batch data exchange processes or online processes such as State Online Query (SOLQ) or Internet SOLQ (SOLQ-I).

The TSSR address management, operational, and technical controls regarding security safeguards to ensure only authorized disclosure and usage of SSA provided information used, maintained, transmitted, or stored by SSA's EIEPs. SSA requires EIEPs to maintain an organizational access control structure that adheres to a three-tiered best practices model. The SSA recommended model is "separation of duties," "need-to-know" and "least privilege."

SSA requires EIEPs to document and notify SSA prior to sharing SSA-provided information with another state entity, or to allow them direct access to their system. **This includes (but not limited to) law enforcement, other state agencies, and state organizations that perform audit, quality, or integrity functions.**

SSA recommends that the EIEP develop and publish a comprehensive Information Technology (IT) Systems Security Policy document that specifically addresses:

- 1) the classification of information processed and stored within the network,
- 2) management, operational, and technical controls to protect the information stored and processed within the network,
- 3) access to the various systems and subsystems within the network,
- 4) Security Awareness Training,

Exhibit E, Attachment B

- 5) Employee and End User Sanctions Policy,
- 6) Contingency Planning and Disaster Recovery

- 7) Incident Response Policy, and

- 8) The disposal of protected information and sensitive documents derived from the system or subsystems on the network.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

**5.2 General System Security Design and Operating Environment
(Planning (PL) Family – (System Security Plan), Contingency Plan (CP)
Family, Physical and Environmental (PE) Family,
NIST SP 800-53 rev. 4)**

In accordance with the NIST suite of Special Publications (SP) (e.g., 800-53, 800-34, etc.), SSA requires the EIEP to maintain policies, procedures, descriptions, and explanations of their overall system design, configuration, security features, and operational environment. They should include explanations of how they conform to SSA's TSSRs. The EIEPs General System Security design and Operating Environment must also address:

- a) the operating environment(s) in which the EIEP will utilize, maintain, store, and transmit SSA-provided information,
- b) the business process(es) in which the EIEP will use SSA-provided information,
- c) the physical safeguards employed to ensure that unauthorized personnel, the public or visitors to the agency cannot access SSA-provided information,
- d) details of how the EIEP keeps audit information pertaining to the use and access to SSA-provided information and associated applications readily available,
- e) electronic safeguards, methods, and procedures for protecting the EIEP's network infrastructure and for protecting SSA-provided information while in transit, in use within a process or application, and at rest ,
- f) a senior management approved Information System Contingency Plan (ISCP) that addresses both internal and external threats. SSA requires the ISCP to include details regarding the organizational business continuity plan (BCP) and a business impact analyses (BIA) that addresses the security of SSA-provided information if a disaster occurs. SSA recommends that state agencies perform disaster exercises at least once annually.,

Exhibit E, Attachment B

- g) how the EIEP prevents unauthorized retrieval of SSA-provided information by computer, remote terminal, or other means; including descriptions of security software other than access control software (e.g., security patch and anti-malware software installation and maintenance, etc.)
- h) how the configurations of devices (e.g., servers, workstations, portable devices) involving SSA-provided information complies with recognized industry standards (i.e. NIST SP's) and SSA's TSSR, and
- i) organizational structure of the agency, number of users, and all external entities that will have access to the system and/or application that displays, transmits, and/or application that displays, transmits and/or stores SSA-provided information.

Note: At its discretion, SSA or a third party (i.e. contractor) must have the option to conduct onsite security reviews or make other provisions, to ensure that EIEPs maintain adequate security controls to safeguard the information we provide.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.3 System Access Control (Access Control (AC) Family, NIST SP 800-53 rev. 4)

EIEPs must utilize and maintain technological (logical) access controls that limit access to SSA-provided information and associated transactions and functions to only those users, processes acting on behalf of authorized users, or devices (including other information systems) authorized for such access based on their official duties or purpose(s). EIEPs must employ a recognized user-access security software package (e.g., RAC-F, ACF-2, TOP SECRET, Active Directory, etc.) or a security software design, which is equivalent to such products. The access control software must employ and enforce (1) PIN/password, and/or (2) PIN/biometric identifier, and/or (3) SmartCard/biometric identifier, etc., (for authenticating users), (and lower case letters, numbers, and special characters; password phrases) for the user accounts of persons, processes, or devices whose functions require access privileges in excess of those of ordinary users.

The EIEP's password policies must require stringent password construction as supported by current NIST guidelines for the user accounts of persons, processes, or devices whose functions require access privileges above those of ordinary users. **SSA strongly recommends Two-Factor Authentication.**

The EIEP's implementation of the control software must comply with recognized industry standards. Password policies should enforce sufficient construction strength (length and complexity) to defeat or minimize risk-based identified vulnerabilities and ensure limitations for password repetition. Technical controls should enforce periodic password changes based on a risk-based standard (e.g., maximum password age of 90 days, minimum password age of 3 – 7 days) and enforce automatic disabling of user accounts that have been inactive for a specified period of time (e.g., 90 days).

The EIEP's password policies must require stringent password construction (e.g., passwords greater than eight characters in length requiring upper and lower case letters, numbers, and/or special characters; password phrases) for the user accounts of persons, processes, or devices whose functions require access privileges in excess of those of ordinary users.

In addition, SSA has the following specific requirements in the area of Access Control:

1. Upon hiring or before granting access to SSA-provided information, EIEPs should verify the identities of any employees, contractors, and agents who will have access to SSA-provided information in accordance with the applicable agency or state's "personnel identity verification policy."
2. SSA requires that state agencies have a logical control feature that designates a maximum number of unsuccessful login attempts for agency workstations and devices that store or process SSA-provided information, in accordance with NIST guidelines. SSA recommends no fewer than three (3) and no greater than five (5)..
3. SSA requires that the state agency designate specific official(s) or functional component(s) to issue PINs, passwords, biometric identifiers, or Personal Identity Verification (PIV) credentials to individuals who will access SSA-provided information. **SSA also requires that the state agency prohibit any functional component(s) or official(s) from issuing credentials or access authority to themselves or other individuals within their job-function or category of access.**
4. SSA requires that EIEPs grant access to SSA-provided information based on least privilege, need-to-know, and separation of duties. State agencies should not routinely grant employees, contractors, or agents access privileges that exceed the organization's business needs. SSA also requires that EIEPs periodically review employees, contractors, and agent's system access to determine if the same levels and types of access remain applicable.
5. If an EIEP employee, contractor, or agent is subject to an adverse administrative action by the EIEP (e.g., reduction in pay, disciplinary action, termination of employment), SSA recommends the EIEP remove his or her access to SSA-provided information in advance of the adverse action to reduce the possibility that will the employee will perform unauthorized activities that involve SSA-provided information.

Exhibit E, Attachment B

6. SSA requires that work-at-home, remote access, and/or Internet access comply with applicable Federal and state security policy and standards. Furthermore, the EIEPs access control policy must define the safeguards in place to adequately protect SSA-provided information for work-at-home, remote access, and/or Internet access.

7. SSA requires EIEPs to design their system with logical control(s) that prevent unauthorized browsing of SSA-provided information. SSA refers to this setup as a **Permission Module**. The term “**Permission Module**” supports a business rule and systematic control that prevents users from browsing a system that contains SSA-provided information. It also supports the principle of **referential integrity**. It should prevent non-business related or unofficial access to SSA-provided information. Before a user or process requests SSA-provided information for verification, the system should verify it is an authorized transaction. Some organizations use the term “referential integrity” to describe the verification step. A properly configured Permission Module should prevent a user from performing any actions not consistent with a need-to-know business process. If a logical permission module configuration is not possible, the state agency must enforce its Access Control List (ACL) in accordance with the principle of least privilege. **The only acceptable compensating control for a system that lacks a permission module is a 100% review of all transactions that involve SSA-provided information.**

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.4 Automated Audit Trail

(Audit and Accountability (AU) Family, NIST SP 800-53 rev. 4)

SSA requires EIEPs, and other STCs or agencies that provide audit trail services to other state agencies that receive information electronically from SSA, to implement and maintain a fully automated audit trail system (ATS). The system must be capable of creating, storing, protecting, and (efficiently) retrieving and collecting records identifying the individual user who initiates a request for information from SSA or accesses SSA-provided information. At a minimum, individual audit trail records must contain the data needed (including date and time stamps) to associate each query transaction or access to SSA-provided information with its initiator, their action, if any, and the relevant business purpose/process (e.g., SSN verification for Medicaid). Each entry in the audit file must be stored as a separate record, not overlaid by subsequent records. The ATS must create transaction files to capture all input from interactive internet applications that access or query SSA-provided information.

SSA requires that the agency's ATS create an audit record when users view screens that contain SSA-provided information. If an STC handles and audits the EIEP's transactions with SSA, the EIEP is responsible for ensuring that the STC's audit capabilities meet NIST's guidelines for an automated audit trail system. The EIEP must also establish a process to obtain specific audit information from the STC regarding the EIEP's SSA transactions.

SSA requires that EIEPs have automated retrieval and collection of audit records. Such automated functions can be via online queries, automated reports, batch processing, or any other logical means of delivering audit records in an expeditious manner. Information in the audit file must be retrievable by an automated method and must allow the EIEP the capability to make them available to SSA upon request.

Access to the audit file must be restricted to authorized users with a "need to know," audit file data must be unalterable (read-only), and maintained for a minimum of three (3) (preferably seven (7)) years. Information in the audit file must be retrievable by an automated method and must allow the EIEP the capability to make them available to SSA upon request. The EIEP must backup audit trail records on a regular basis to ensure its availability. EIEPs must apply the same level of protection to backup audit files that apply to the original files to ensure the integrity of the data.

If the EIEP retains SSA-provided information in a database (e.g., Access database, SharePoint, etc.), or if certain data elements within the EIEP's system indicates to users that SSA verified the information, the EIEP's system must also capture an audit trail record of users who view SSA-provided information stored within the EIEP's system. The retrieval requirements for SSA-provided information at rest and the retrieval requirements for regular transactions are identical. **Similar to the Permission Module requirement above, the only acceptable compensating control for a system that lacks an Automated Audit Trail System (ATS) is a 100% review of all transactions that involve SSA-provided information.**

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.5 Personally Identifiable Information (PII)

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and AP Family – Authority and Purpose (Privacy Controls), NIST SP 800-53 rev. 4)

Personally Identifiable Information (PII) is information used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, alone or when combined with other personal or identifying information linked or linkable to a specific individual. An item such as date and place of birth, mother's maiden name, or father's surname is PII, regardless of whether combined with other data.

SSA defines a **PII loss** as a circumstance when an EIEP employee, contractor, or agent has reason to believe that information on hard copy or in electronic format, which contains PII provided by SSA, left the EIEP's custody or the EIEP disclosed it to an unauthorized individual or entity. PII loss is a reportable incident. SSA requires that contracts for periodic disposal/destruction of case files or other print media contain a non-disclosure agreement signed by all personnel who will encounter products that contain SSA-provided information.

If a PII loss involving SSA-provided information occurs or is suspected, the EIEP must be able to quantify the extent of the loss and compile a complete list of the individuals potentially affected by the incident (refer to [Incident Reporting](#)).

The EIEP should have procedural documents to describe methods and controls for safeguarding SSA-provided PII while in use, at rest, during transmission, or after archiving. The document should explain how the EIEP manages and handles SSA-provided information on print media and explain how the methods and controls conform to NIST requirements. SSA requires that printed items that contain SSA-provided PII always remain in the custody of authorized EIEP employees, contractors, or agents. SSA also requires that the agency destroy the items when no longer required for the EIEP's business process. If retained in paper files for evidentiary purposes, the EIEP should safeguard such PII in a manner that prevents unauthorized personnel from accessing such materials. All agencies that receive SSA-provided information must maintain an inventory of all documents that outline statewide or agency policy and procedures regarding the same.

5.6 Monitoring and Anomaly Detection

(Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST SP 800-137, E-Government Act of 2002 (P.L. 107-347), and Security Assessment and Authorization (CA) and Risk Assessment (RA) Families, NIST SP 800-53 rev. 4)

SSA requires that the EIEPs use an Intrusion Protection System (IPS) or an Intrusion Detection System (IDS). The EIEP must establish and/or maintain continuous monitoring of its network infrastructure and assets to ensure that:

- 1) the EIEP's security controls continue to be effective over time,
- 2) the EIEP uses industry-standard Security Information Event Manager (SIEM) tools, anti-malware software, and effective antivirus protection,
- 3) only authorized individuals, devices, and processes have access to SSA-provided information,
- 4) the EIEP detects efforts by external and internal entities, devices, or processes to perform unauthorized actions (e.g., data breaches, malicious attacks, access to network assets, software/hardware installations, etc.) as soon as they occur,
- 5) the necessary parties are immediately alerted to unauthorized actions performed by external and internal entities, devices, or processes,
- 6) upon detection of unauthorized actions, measures are immediately initiated to prevent or mitigate associated risk,
- 7) in the event of a data breach or security incident, the EIEP can efficiently determine and initiate necessary remedial actions, and
- 8) trends, patterns, or anomalous occurrences and behavior in user or network activity that may be indicative of potential security issues are readily discernible.

The EIEP's system must include the capability to prevent users from unauthorized browsing of SSA records. SSA requires the use of a transaction-driven **permission module design**, whereby employees are unable to initiate transactions not associated with the normal business process. If the EIEP uses such a design, they also must have anomaly detection to monitor an employee's unauthorized attempts to gain access to SSA-provided information and attempts to obtain information from SSA for clients not in the EIEP's client system. The EIEP should employ measures to ensure the permission module's integrity. Users should not be able to create a bogus case and subsequently delete it in such a manner that it goes undetected. The SSA permission module design employs both role and rules based logical access control restrictions. (Refer to [Access Control](#))

If the EIEP's design **does not use** a permission module **and** is not transaction-driven, until at least one of these security features exists, the EIEP must develop and implement **compensating security controls** to deter employees from browsing SSA records. These controls must include monitoring and anomaly detection features, such as: systematic, manual, or a combination thereof. Such features must include the capability to detect anomalies in the volume and/or type of transactions or queries requested or initiated by individuals and include systematic or manual procedures for verifying that requests and queries of SSA-provided information comply with valid official business purposes.

Risk Management Program

SSA recommends that EIEPs develop and maintain a published Risk Assessment Policy and Procedures document. A Risk Management Program may include, but is not limited to the following:

1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance,
2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls,
3. A function that 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,
4. An independent function that conducts vulnerability and risk assessments, reviews risk assessment results, and disseminates such information to senior management,
5. A firm commitment from senior management to update the risk assessment whenever there are significant changes to the information

system or environment of operation or other conditions that may affect the security of SSA-provided information,

6. A robust vulnerability scanning protocol that employs industry standard scanning tools and techniques that facilitate interoperability among tools and automates parts of the vulnerability management process,
7. Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk, and
8. Shares information obtained from the vulnerability scanning process and security control assessments with senior management to help eliminate similar vulnerabilities in other information systems that receive, process, transmit, or store SSA-provided information.

Note: The EIEP's decision to initiate or maintain an official Risk Management Program and establish a formal Risk Assessment Strategy for mitigating risk is strictly voluntary, but highly recommended by SSA.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.7 Management Oversight and Quality Assurance

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the AC – Access Control & PM – Program Management Families, NIST SP 800-53 rev. 4)

SSA requires the EIEP to establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized users have access to SSA-provided information. This will ensure there is ongoing compliance with the terms of the EIEP's electronic information sharing agreement with SSA and the TSSRs established for access to SSA-provided information. The entity responsible for management oversight should consist of one or more of the EIEP's management officials whose job functions include responsibility to ensure that the EIEP only grants access to the appropriate users and position types (least privilege), which require the SSA-provided information to do their jobs (need-to-know).

SSA requires the EIEP to ensure that users granted access to SSA-provided information receive adequate training on the sensitivity of the information, associated safeguards, operating procedures, and the civil and criminal consequences or penalties for misuse or improper disclosure.

SSA requires that EIEPs establish the following job functions and require that only users whose job functions are separate from personnel who request or use SSA-provided information.

SSA requires that EIEPs establish the following job functions separate from personnel who request or use SSA-provided information.

- a) Perform periodic self-reviews to monitor the EIEP's ongoing usage of SSA-provided information.
- b) Perform random sampling of work activity that involves SSA-provided information to determine if the access and usage comply with SSA's requirements

SSA requires the EIEP's system to produce reports that allow management and/or supervisors to monitor user activity. The EIEP must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors or to local security officers. The process must ensure that only those whose responsibilities include monitoring anomalous activity of users, to include those who have exceptional system rights and privileges, use the reports.

1. User ID Exception Reports:

This type of report captures information about users who enter incorrect user IDs when attempting to gain access to the system or to a transaction that initiates requests for information from SSA, including failed attempts to enter a password.

2. Inquiry Match Exception Reports:

This type of report captures information about users who initiate transactions for SSNs that have no client case association within the EIEP's system **(the EIEP's management must review 100% of these cases)**.

3. System Error Exception Reports:

This type of report captures information about users who may not understand or may be violating proper procedures for access to SSA-provided information.

4. Inquiry Activity Statistical Reports:

This type of report captures information about transaction usage patterns among authorized users and is a tool that enables the EIEP's management to monitor typical usage patterns in contrast to extraordinary usage patterns.

The EIEP must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors or to local security officers. The process must ensure that only those whose responsibilities include monitoring anomalous activity of users, to include those who have exceptional system rights and privileges, use the reports.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.8 Data and Communications Security

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the Access Control (AC), Configuration Management (CM), Media Protection (MP), and System and Communication (SC) Families, NIST SP 800-53 rev. 4)

SSA requires EIEPs to encrypt PII and SSA-provided information when transmitting across dedicated communications circuits between its systems, intrastate communications between its local office locations, and on the EIEP's mobile computers, devices and removable media. The EIEP's encryption methods must align with the Guidelines established by the National Institute of Standards and Technology (NIST). SSA recommends the Advanced Encryption Standard (AES) or Triple DES (Data Encryption Standard 3).

Files encrypted for external users (when using tools such as Microsoft Word encryption,) require a key length of at least nine characters. SSA recommends that the key (also referred to as a password) contain both special characters and numbers. SSA supports the NIST Guidelines that requires the EIEP deliver the key so that it does not accompany the media. The EIEP must secure the key when not in use or unattended.

SSA discourages the use of the public Internet for transmission of SSA-provided information. If, however, the EIEP uses the public Internet or other electronic communications, such as emails and faxes to transmit SSA-provided information, they must use a secure encryption protocol such as Secure Socket Layer (SSL) or Transport Layer Security (TLS). SSA also recommends 256-bit encryption protocols or more secure methods such as Virtual Private Network technology. The EIEP should only send data to a secure address or device to which the EIEP can control and limit access to only specifically authorized individuals and/or processes. **SSA recommends that EIEPs use Media Access Control (MAC) Filtering and Firewalls to protect access points from unauthorized devices attempting to connect to the network.**

EIEPs should not retain SSA-provided information any longer than business purpose(s) dictate. The IEA with SSA stipulates a time for data retention. The EIEP should delete, purge, destroy, or return SSA-provided information when the business purpose for retention no longer exists.

The EIEP may not save or create separate files comprised solely of information provided by SSA. The EIEP may apply specific SSA-provided information to the EIEP's matched record from a preexisting data source. Federal law prohibits duplication and redisclosure of SSA-provided information without written approval from SSA.

This prohibition applies to both internal and external sources who do not have a “need-to-know.” SSA recommends that EIEPs use either **Trusted Platform Module (TPM)** or **Hardware Security Module (HSM)** technology solutions to encrypt data at rest on hard drives and other data storage media.

SSA requires EIEPs to prevent unauthorized disclosure of SSA-provided information after they complete processing and after the EIEP no longer requires the information. The EIEP’s operational processes must ensure that no residual SSA-provided information remains on the hard drives of user’s workstations after the user exits the application(s) that use SSA-provided information. If the EIEP must send a computer, hard drive, or other computing or storage device offsite for repair, the EIEP must have a non-disclosure clause in their contract with the vendor. If the EIEP used the item in connection with a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect the EIEP’s vendor contract. The EIEP must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects the EIEP to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.

To sanitize media, the EIEP should use one of the following methods:

1. Overwriting/Clearing:

Overwrite utilities can only be used on working devices. Overwriting is appropriate only for devices designed for multiple reads and writes. The EIEP should overwrite disk drives, magnetic tapes, floppy disks, USB flash drives, and other rewriteable media. The overwrite utility must completely overwrite the media. SSA recommends the use of purging media sanitization to make the data irretrievable, protecting data against laboratory attacks or forensics. Reformatting the media does not overwrite the data.

2. Degaussing:

Degaussing is a sanitization method for magnetic media (e.g., disk drives, tapes, floppies, etc.). Degaussing is not effective for purging non-magnetic media (e.g., optical discs). SSA and NIST Guidelines require EIEP to use a certified tool designed to degauss each particular type of media. NIST guidelines require certification of the tool to ensure that the magnetic flux applied to the media is strong enough to render the information irretrievable. The degaussing process must render data on the media irretrievable by a laboratory attack or laboratory forensic procedures.

3. **Physical destruction:**

NIST guidelines require physical destruction when degaussing or overwriting cannot be accomplished (for example, CDs, floppies, DVDs, damaged tapes, hard drives, damaged USB flash drives, etc.). Examples of physical destruction include shredding, pulverizing, and burning.

State agencies may retain SSA-provided information in hardcopy only if required to fulfill evidentiary requirements, provided the agencies retire such data in accordance with applicable state laws governing state agency's retention of records. The EIEP must control print media containing SSA-provided information to restrict access to authorized employees who need such access to perform official duties. EIEPs must destroy print media containing SSA-provided information in a secure manner when no longer required for business purposes. SSA requires the EIEP to destroy paper documents that contain SSA-provided information by burning, pulping, shredding, macerating, or other similar means that ensure the information is unrecoverable.

State agencies may use any accretions, deletions, or changes to the SSA-provided information governed by the CMPPA agreement to update their master files or federally funded state-administered benefit program applicants and recipients and retain such master files in accordance with applicable state laws governing State Agencies' retention of records.

NOTE: Hand tearing or lining through documents to obscure information does not meet SSA's requirements for appropriate destruction of PII.

The EIEP must employ measures to ensure that communications and data furnished to SSA contain no viruses or other malware.

Special Note regarding Cloud Service Providers:

If the EIEP will store SSA-provided information through a Cloud Service Provider, please provide the name and address of the cloud provider. Describe the security responsibilities the contract requires to protect SSA-provided information.

SSA will ask for detailed descriptions of the security features contractually required of the cloud provider and information regarding how they will protect SSA-provided information at rest and when in transit.

EIEPs cannot legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.9 Incident Reporting

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the Incident Response (IR) Family, NIST SP 800-53 rev. 4)

FISMA, NIST Guidelines, and Federal Law require the EIEP to develop and implement policies and procedures to respond to potential data breaches or PII losses. EIEPs must articulate, in writing, how the policies and procedures conform to SSA's requirements. The procedures must include the following information:

*If your agency experiences or suspects a breach or loss of PII or a security incident, which includes SSA-provided information, they must notify the State official responsible for Systems Security designated in the agreement. That State official or delegate must then notify the SSA Regional Office Contact or the SSA Systems Security Contact identified in the agreement. If, for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact **within one hour**, the responsible State Agency official or delegate must report the incident by contacting **SSA's National Network Service Center (NNSC) toll free at 877-697-4889** (select "Security and PII Reporting" from the options list). The EIEP will provide updates as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.*

If SSA, or another Federal investigating entity (e.g. TIGTA or DOJ), determines that the risk presented by a breach or security incident requires that the state agency notify the subject individuals, the agency must agree to absorb all costs associated with notification and remedial actions connected to security breaches. **SSA and NIST Guidelines encourage agencies to consider establishing incident response teams to address PII and SSA-provided information breaches.**

Incident reporting policies and procedures are part of the security awareness program. Incident reporting pertains to all employees, contractors, or agents regardless as to whether they have direct responsibility for contacting SSA. The written policy and procedures document should include specific names, titles, or functions of the individuals responsible for each stage of the notification process. The document should include detailed instructions for how, and to whom each employee, contractor, or agent should report the potential breach or PII loss.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.10 Security Awareness Training and User Sanctions

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and Awareness and Training (AT), Personnel Security (PS), and Program Management (PM) Families, NIST SP 800-53 rev. 4)

The EIEP must have an active and robust security awareness program and security training for all employees, contractors, and agents who access SSA-provided information. The training and awareness programs must include:

- a. the sensitivity of SSA-provided information and addresses the Privacy Act and other Federal and state laws governing its use and misuse,
- b. the rules of behavior concerning use and security in systems and/or applications processing SSA-provided information,
- c. the restrictions on viewing and/or copying SSA-provided information,
- d. the responsibilities of employees, contractors, and agent's pertaining to the proper use and protection of SSA-provided information,
- e. the proper disposal of SSA-provided information,
- f. the security breach and data loss incident reporting procedures,
- g. the basic understanding of procedures to protect the network from malware attacks,
- h. spoofing, phishing and pharming, and network fraud prevention, and
- i. the possible criminal and civil sanctions and penalties for misuse of SSA-provided information.

SSA requires the EIEP to provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. SSA also requires the EIEP to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful access and/or disclosure.

Exhibit E, Attachment B

SSA requires the EIEP to provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. SSA also requires the EIEP to certify that each employee, contractor, or agent who views SSA-provided information also certify that they understand the potential criminal and administrative sanctions or penalties for unlawful disclosure. SSA requires the state agency to require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. The non-disclosure attestation must also include acknowledgement from each employee, contractor, and agent that he or she understands and accepts the potential criminal and/or civil sanctions or penalties associated with misuse or unauthorized disclosure of SSA-provided information. The state agency must retain the non-disclosure attestations for at least five (5) to seven (7) years for each individual who processes, views, or encounters SSA-provided information as part of their duties.

SSA strongly recommends the use of login banners, emails, posters, signs, memoranda, special events, and other promotional materials to encourage security awareness throughout your enterprise.

The state agency must designate a department or party to take the responsibility to provide ongoing security awareness training for all employees, contractors, and agents who access SSA-provided information. Training must include:

- The sensitivity of SSA-provided information and address the Privacy Act and other Federal and state laws governing its use and misuse
- Rules of behavior concerning use and security in systems processing SSA-provided information
- Restrictions on viewing and/or copying SSA-provided information
- The employee, contractor, and agent's responsibility for proper use and protection of SSA-provided information
- Proper disposal of SSA-provided information
- Security incident reporting procedures
- Basic understanding of procedures to protect the network from malware attacks

- Spoofing, Phishing and Pharming scam prevention
- The possible sanctions and penalties for misuse of SSA-provided information

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.11 Contractors of Electronic Information Exchange Partners
(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and Risk Assessment (RA), System and Services Acquisition (SA), Awareness and Training (AT), Personnel Security (PS), and Program Management (PM) Families, NIST SP 800-53 rev. 4)

The state agency's employees, contractors, and agents who access, use, or disclose SSA data in a manner or purpose not authorized by the Agreement may be subject to both civil and criminal sanctions pursuant to applicable Federal statutes. The state agency will provide its contractors and agents with copies of the Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing the Agreement, and thereafter at SSA's request, the state agency will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to SSA data and provide such lists to SSA.

Contractors of the state agency must adhere to the same security requirements as employees of the state agency. The state agency is responsible for the oversight of its contractors and the contractor's compliance with the security requirements. The state agency must enter into a written agreement with each of its contractors and agents who need SSA data to perform their official duties. Such contractors or agents agree to abide by all relevant Federal laws, restrictions on access, use, disclosure, and the security requirements contained within the state agency's agreement with SSA.

The state agency must provide proof of the contractual agreement with all contractors and agents who encounter SSA-provided information as part of their duties. If the contractor processes, handles, or transmits information provided to the state agency by SSA or has authority to perform on the state agency's behalf, the state agency should clearly state the specific roles and functions of the contractor within the agreement. The state agency will provide SSA written certification that the contractor is meeting the terms of the agreement, including SSA security requirements. The service level agreements with the contractors and agents must contain non-disclosure language as it pertains to SSA-provided information.

The state agency must also require that contractors and agents who will process, handle, or transmit information provided to the state agency by SSA to include language in their signed agreement that obligates the contractor to follow the terms of the state agency's data exchange agreement with SSA. The state agency must also make certain that the contractor and agent's employees receive the same security awareness training as the state agency's employees. The state agency, the contractor, and the agent should maintain awareness-training records for their employees and require the same mandatory annual

certification procedures.

SSA requires the state agency to subject the contractor to ongoing security compliance reviews that must meet SSA standards. The state agency will conduct compliance reviews at least triennially commencing no later than three (3) years after the approved initial security certification to SSA. The state agencies will provide SSA with documentation of their recurring compliance reviews of their contractors and agents. The state agencies will provide the documentation to SSA during their scheduled compliance and certification reviews or upon SSA's request.

If the state agency's contractor will be involved with the processing, handling, or transmission of information provided to the EIEP by SSA offsite from the EIEP, the EIEP must have the contractual option to perform onsite reviews of that offsite facility to ensure that the following meet SSA's requirements:

- a) safeguards for sensitive information,
- b) technological safeguards on computer(s) that have access to SSA-provided information,
- c) security controls and measures to prevent, detect, and resolve unauthorized access to, use of, and redisclosure of SSA-provided information, and
- d) continuous monitoring of the EIEP contractors or agent's network infrastructures and assets.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.12 Cloud Service Providers (CSP) for Electronic Information Exchange Partners

(NIST SP 800-144, NIST SP 800-145, NIST SP 800-146, OMB Memo M-14-03, NIST SP 137)

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145 defines Cloud Computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.” The three service models, as defined by NIST SP 800-145 are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The Deployment models are Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud. Furthermore, The Federal Risk and Authorization Program (FedRAMP) is a risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

SSA requires the State Agency, contractor(s), and agent(s) to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.

SSA requires the State Agency, contractor(s), and agent(s) to agree that any state-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a “de facto” extension of the State Agency and is subject to onsite inspection and review by the State Agency or SSA with prior notice.

SSA requires that the State Agency thoroughly describe all specific contractual obligations of each party to the Cloud Service Provider (CSP) agreement between the state agency and the CSP vendor(s). If the obligations, services, or conditions widely differ from agency to agency, we require separate SDP Questionnaires to address the CSP services provided to each state agency involved in the receipt, processing, storage, or disposal of SSA-provided information.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6. Security Certification and Compliance Review Programs
(NIST SP 800-18 – System Security Plans and Planning (PL) Family, NIST SP 800-53 rev. 4)

SSA's security certification and compliance review programs are distinct processes. The certification program is a unique episodic process when an EIEP initially requests electronic access to SSA-provided information or makes substantive changes to existing exchange protocol, delivery method, infrastructure, or platform. The certification process entails two stages (refer to 6.1 for details) intended to ensure that management, operational, and technical security measures work as designed. SSA must ensure that the EIEPs fully conform to SSA's security requirements at the time of certification and satisfy both stages of the certification process before SSA will permit online access to its data in a production environment.

The compliance review program entails cyclical security review of the EIEP performed by, or on behalf of SSA. The purpose of the review is to assess an EIEP's conformance to SSA's current security requirements at the time of the review engagement. The compliance review program applies to both online and batch access to SSA-provided information. Under the compliance review program, EIEPs are subject to ongoing and periodic security reviews by SSA.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.1 The Security Certification Program
(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

The security certification process applies to EIEPs that seek online electronic access to SSA-provide information and consists of two general phases:

- a) **Phase 1:** The Security Design Plan (SDP) is a formal written plan authored by the EIEP to document its management, operational, and technical security controls to safeguard SSA-provided information (refer to [Documenting Security Controls in the Security Design Plan](#)).

NOTE: SSA may have legacy EIEPs (EIEPs not certified under the current process) who have not prepared an SDP. SSA strongly recommends that these EIEPs prepare an SDP.

The EIEP's preparation and maintenance of a current SDP will aid them in determining potential compliance issues prior to reviews, assuring continued compliance with SSA's TSSRs, and providing for more efficient security reviews.

- b) **Phase 2:** The SSA Onsite Certification is a formal security review conducted by SSA, or on its behalf, to examine the full suite of management, operational, and technical security controls implemented by the EIEP to safeguard data obtained from SSA electronically (refer to [The Certification Process](#)).

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.2 Documenting Security Controls in the SDP

(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

6.2.1 When an SDP is required:

EIEPs must submit an SDP when one or more of the following circumstances apply:

- a) to obtain approval for requested access to SSA-provided information for an initial agreement,
- b) to obtain approval to reestablish previously terminated access to SSA-provided information,
- c) to obtain approval to implement a new operating or security platform that will involve SSA-provided information,
- d) to obtain approval for significant changes to the EIEP's organizational structure, technical processes, operational environment, or security implementations planned or made since approval of their most recent SDP or of their most recent successfully completed security review,
- e) to confirm compliance when one or more security breaches or incidents involving SSA-provided information occurred since approval of the EIEP's most recent SDP or of their most recent successfully completed security review,
- f) to document descriptions and explanations of measures implemented as the result of a data breach or security incident,
- g) to document descriptions and explanations of measures implemented to resolve non-compliance issue(s), and
- h) to obtain a new approval after SSA revoked approval of the most recent SDP

SSA may require a new SDP if changes occurred (other than those listed above) that may affect the terms of the EIEP's data exchange agreement with SSA.

SSA will not approve the SDP or allow the initiation of transactions and/or access to SSA-provided information before the EIEP complies with the TSSRs.

NOTE: EIEPs that function only as an STC, transferring SSA-provided information to other EIEPs must, per the terms of their agreements with SSA, adhere to SSA's TSSR and exercise their responsibilities regarding protection of SSA-provided information. (See Page 48 Definition of STC)

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.3 The Certification Process

(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

Once the EIEP has successfully satisfied Phase 1, SSA will conduct an onsite certification review. The objective of the onsite review is to ensure the EIEP's management, operational, and technical controls safeguarding SSA-provided information from misuse and improper disclosure and that those safeguards function and work as intended.

At its discretion, SSA may request the EIEP to participate in an onsite review and compliance certification of their security infrastructure.

The onsite review may address any or all of SSA's security requirements and include, when appropriate:

- 1) a demonstration of the EIEP's implementation of each security requirement,
- 2) a physical review of pertinent supporting documentation to verify the accuracy of responses in the SDP,
- 3) a demonstration of the functionality of the software interface for the system that will receive, process, and store SSA-provided information,
- 4) a demonstration of the Automated Audit Trail System (ATS),
- 5) a walkthrough of the EIEP's data center to observe and document physical security safeguards,
- 6) a demonstration of the EIEP's implementation of electronic exchange of data with SSA,
- 7) a discussions with managers, supervisors, information security officers, system administrators, or other state stakeholders,
- 8) an examination of management control procedures and reports pertaining to anomaly detection or anomaly prevention,
- 9) a demonstration of technical tools pertaining to user access control and, if appropriate, browsing prevention,

- 10) a demonstration of the permission module or similar design, to show how the system triggers requests for information from SSA,
- 11) a demonstration of how the process for requests for SSA-provided information prevents SSNs not present in the EIEP's system from sending requests to SSA.

We may attempt to obtain information from SSA using at least one, randomly created, fictitious number not known to the EIEPs system.

During a certification or compliance review, SSA or a certifier acting on its behalf, may request a demonstration of the EIEP's ATS and its record retrieval capability. SSA or a certifier may request a demonstration of the ATS' capability to track the activity of employees who have the potential to access SSA-provided information within the EIEP's system. The certifier may request more information from those EIEPs who use an STC to handle and audit transactions. SSA or a certifier may conduct a demonstration to see how the EIEP obtains audit information from the STC regarding the EIEP's SSA transactions.

If an STC handles and audits an EIEP's transactions, SSA requires the EIEP to demonstrate both their in-house audit capabilities and the process used to obtain audit information from the STC.

If the EIEP employs a contractor or agent who processes, handles, or transmits the EIEP's SSA-provided information offsite, SSA, at its discretion, may request to include the contractor's facility in the onsite certification review. The inspection may occur with or without a representative of the EIEP.

Upon successful completion of the onsite certification review, SSA will authorize electronic access to production data by the EIEP. SSA will provide written notification of its certification to the EIEP and all appropriate internal SSA components.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.5 The Compliance Review Program and Process
(NIST SP 800-18 – System Security Plans, Configuration Management (CM), Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

Similar to the certification process, the compliance review program entails a process intended to ensure that EIEPs that receive electronic information from SSA are in full compliance with the SSA's TSSRs. SSA requires EIEPs to complete and submit (based on a timeline agreed upon by SSA and EIEP's stakeholders) a Compliance Review Questionnaire (CRQ). The CRQ (similar to the SDP), describes the EIEP's management, operational, and technical controls used to protect SSA-provided information from misuse and improper disclosure. We also want to verify that those safeguards function and work as intended.

As a practice, SSA attempts to conduct compliance reviews following a 3-5 year periodic review schedule. However, as circumstances warrant, a review may take place at any time. Three prominent examples that would trigger an ad hoc review are:

- A. a significant change in the outside EIEP's computing platform,
- B. a violation of any of SSA's TSSRs, or
- C. an unauthorized disclosure of SSA-provided information by the EIEP.

SSA may conduct onsite compliance reviews and include both the EIEP's main facility and a field office.

SSA may, at its discretion, request that the EIEP participate in an onsite compliance review of their security infrastructure to confirm the implementation of SSA's security requirements.

The onsite review may address any or all of SSA's security requirements and include, where appropriate:

- D. a demonstration of the EIEP's implementation of each requirement
- E. a random sampling of audit records and transactions submitted to SSA
- F. a walkthrough of the EIEP's data center to observe and document physical security safeguards
- G. a demonstration of the EIEP's implementation of online exchange of data with SSA,

- H. a discussion with managers, supervisors, information security officers, system administrators, or other state stakeholders,
 - I. an examination of management control procedures and reports pertaining to anomaly detection and prevention reports,
 - J. a demonstration of technical tools pertaining to user access control and, if appropriate, browsing prevention,
 - K. a demonstration of how a permission module or similar design triggers requests for information from SSA, and
 - L. a demonstration of how a permission module prevents the EIEP's system from processing SSNs not present in the EIEP's system.
- 1) We can accomplish this by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the EIEP's system.**

SSA may perform an onsite or remote review for reasons including, but not limited, to the following:

- a) the EIEP has experienced a security breach or incident involving SSA-provided information
- b) the EIEP has unresolved non-compliance issue(s)
- c) to review an offsite contractor's facility that processes SSA-provided information
- d) the EIEP is a legacy organization that has not yet been through SSA's security certification and compliance review programs
- e) the EIEP requested that SSA perform an IV & V (Independent Verification and Validation review)

During the compliance review, SSA, or a certifier acting on its behalf, may request a demonstration of the system's audit trail and retrieval capability. The certifier may request a demonstration of the system's capability for tracking the activity of employees who view SSA-provided information within the EIEP's system. The certifier may request EIEPs that have STCs that handle and audit transactions with SSA to demonstrate the process used to obtain audit information from the STC.

If an STC handles and audits the EIEP's transactions with SSA, we may require the EIEP to demonstrate both their in-house audit capabilities and the processes used to

obtain audit information from the STC regarding the EIEP's transactions with SSA.

If the EIEP employs a contractor who will process, handle, or transmit the EIEP's SSA-provided information offsite, SSA, at its discretion, may request to include in the onsite compliance review an onsite inspection of the contractor's facility. The inspection may occur with or without a representative of the EIEP. The format of the review in routine circumstances (e.g., the compliance review is not being conducted to address a special circumstance, such as a disclosure violation, etc.) will generally consist of reviewing and updating the EIEP's compliance with the systems security requirements described above in this document. At the conclusion of the review, SSA will issue a formal report to appropriate EIEP personnel. The Compliance Report will address findings and recommendations from SSA's compliance review, which includes a plan for monitoring each issue until closure.

NOTE: SSA will never request documentation for compliance reviews unless necessary to assess the EIEP's security posture. The information is only accessible to authorized individuals who have a need for the information as it relates to the EIEP's compliance with its electronic data exchange agreement with SSA and the associated system security requirements and procedures. SSA will not retain the EIEP's documentation any longer than required. SSA will delete, purge, or destroy the documentation when the retention requirement expires.

Compliance Reviews are either on-site or remote reviews. High-risk reviews must be onsite reviews, medium risk reviews are usually onsite, and low risk reviews may qualify for a remote review via telephone. The past performance of the entire state determines whether a review is onsite or remote **SSA determines a state's risk level based on the "high water mark principle."** If one agency is high risk, the entire state is high risk. The following is a high-level example of the analysis that aids SSA in making a preliminary determination as to which review format is appropriate. SSA may also use additional factors to determine whether SSA will perform an onsite or remote compliance review.

A. High/Medium Risk Criteria

- 1) undocumented closing of prior review finding(s),
- 2) implementation of management, operational or technical controls that affect security of SSA-provided information (e.g. implementation of new data access method), or
- 3) a reported PII breach within the state.

B. Low Risk Criteria

- 1) no prior review finding(s) or prior finding(s) documented as closed
- 2) no implementation of technical/operational controls that impact security of SSA provided
- 3) information (e.g. implementation of new data access method) no reported PII breach

6.5.1 EIEP Compliance Review Participation

SSA may request to meet with the following stakeholders during the compliance review:

- a) a sample of managers, supervisors, information security officers, system administrators, etc. responsible for enforcing and monitoring ongoing compliance to security requirements and procedures to assess their level of training to monitor their employee's use of SSA-provided information, and for reviewing reports and taking necessary action
- b) the individuals responsible for performing security awareness and employee sanction functions to learn how EIEPs fulfill this requirement
- c) a sample of the EIEP's employees to assess their level of training and understanding of the requirements and potential sanctions applicable to the use and misuse of SSA-provided information
- d) the individual(s) responsible for management oversight and quality assurance functions to confirm how the EIEP accomplishes this requirement
- e) any additional individuals as deemed appropriate by SSA (i.e. analysts, Project/Program Manager, claims reps, etc.)

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.6 Scheduling the Onsite Review

SSA will not schedule the onsite review until SSA approves the EIEP's SDP or the EIEPs stakeholders participating in the compliance review have agreed upon a schedule. There is no prescribed period for arranging the subsequent onsite review (*certification review* for an EIEP requesting initial access to SSA-provided information for an initial agreement or *compliance review* for other EIEPs). Unless there are compelling circumstances precluding it; the onsite review will occur as soon as reasonably possible.

The scheduling of the onsite review may depend on additional factors including:

- a) the reason for submission of an SDP or CRQ,
- b) the severity of security issues, if any,
- c) circumstances of the previous review, if any, and
- d) SSA's workload and resource considerations.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

7. Additional Definitions

Back Button:

Refers to a button on a web browser's toolbar, the *backspace button* on a computer keyboard, a programmed keyboard button or mouse button, etc., that returns a user to a previously visited web page or application screen.

Breach:

Refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where unauthorized persons have access or potential access to PII or Covered Information, whether physical, electronic, or in spoken word or recording

Browsing:

Requests for or queries of SSA-provided information for purposes not related to the performance of official job duties

Choke Point:

The firewall between a local network and the Internet is a choke point in network security, because any attacker would have to come through that channel, which is typically protected and monitored.

Cloud Computing:

The term refers to Internet-based computing derived from the cloud drawing representing the Internet in computer network diagrams. Cloud computing providers deliver on-line and on-demand Internet services. Cloud Services normally use a browser or Web Server to deliver and store information.

Cloud Computing (NIST SP 800-145 Excerpt):

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics:

On-demand self-service - A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access - Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling - The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity - Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service - Cloud systems automatically control and optimize resource use by leveraging a metering capability¹ at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

Software as a Service (SaaS) - The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure². The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS) - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.³ The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS) - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

Private cloud - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud - The cloud infrastructure is provisioned for exclusive use by a specific

community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

1 Typically this is done on a pay-per-use or charge-per-use basis.

2 A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

3 This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.

Cloud Drive:

A cloud drive is a Web-based service that provides storage space on a remote server.

Cloud Audit:

Cloud Audit is a specification developed at Cisco Systems, Inc. that provides cloud computing service providers a standard way to present and share detailed, automated statistics about performance and security.

The Federal Risk and Authorization Program (FedRAMP):

FedRAMP is a risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

Commingling:

Commingling is the creation of a common database or repository that stores and maintains both SSA-provided information and preexisting EIEP PII.

Data Exchange:

Data Exchange is a logical transfer of information from one government entity's systems of records (SOR) to another agency's application or mainframe through a secure and exclusive connection.

Degaussing:

Degaussing is the method of using a "special device" (i.e., a device that generates a magnetic field) in order to disrupt magnetically recorded information. Degaussing can be effective for purging damaged media and media with exceptionally large storage capacities. Degaussing is not effective for purging non-magnetic media (e.g., optical discs).

Function:

One or more persons or organizational components assigned to serve a particular purpose, or perform a particular role. The purpose, activity, or role assigned to one or more persons or organizational components.

Hub:

As it relates to electronic data exchange with SSA, a hub is an organization, which serves as an electronic information conduit or distribution collection point. The term Hub is interchangeable with the terms "State Transmission Component," "State Transfer Component," or "STC."

ICON:

Interstate Connection Network (various entities use 'Connectivity' rather than 'Connection')

IV & V:

Independent Verification and Validation

Legacy System:

A term usually referring to a corporate or organizational computer system or network that utilizes outmoded programming languages, software, and/or hardware that typically no longer receives support from the original vendors or developers.

Manual Transaction:

A user-initiated operation (also referred to as a "user-initiated transaction"). This is the opposite of a system-generated automated process.

Example: A user enters a client's information including the client's SSN and presses the "ENTER" key to acknowledge that input of data is complete. A new screen appears with multiple options, which include "VERIFY SSN" and "CONTINUE". The user has the option to verify the client's SSN or perform alternative actions.

Media Sanitization:

- f) Disposal: Refers to the discarding (e.g., recycling) media that contains no sensitive or confidential data.
- g) Overwriting/Clearing: This type of media sanitization is adequate for protecting information from a robust keyboard attack. Clearing must prevent retrieval of information by data, disk, or file recovery utilities. Clearing must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. For example, overwriting is an acceptable method for clearing media. Deleting items, however, is not sufficient for clearing.

This process may include overwriting all addressable locations of the data, as well as its logical storage location (e.g., its file allocation table). The aim of the overwriting process is to replace or obfuscate existing information with random data. Most rewriteable media may be cleared by a single overwrite. This method of sanitization is not possible on unwriteable or damaged media.

- h) Purging: This type of media sanitization is a process that protects information from a laboratory attack. The terms *clearing* and *purging* are sometimes synonymous. However, for some media, clearing is not sufficient for purging (i.e., protecting data from a laboratory attack). Although most re-writeable media requires a single overwrite, purging may require multiple rewrites using different characters for each write cycle.

This is because a laboratory attack involves threats with the capability to employ non-standard assets (e.g., specialized hardware) to attempt data recovery on media outside of that media's normal operating environment.

- i) Degaussing is also an example of an acceptable method for purging magnetic media. The EIEP should destroy media if purging is not a viable method for sanitization.
- Destruction: Physical destruction of media is the most effective form of sanitization. Methods of destruction include burning, pulverizing, and shredding. Any residual medium should be able to withstand a laboratory attack.

Permission module:

A utility or subprogram within an application, which automatically enforces the relationship of a request for or query of SSA-provided information to an authorized process or transaction before initiating a transaction. The System will not allow a user to request information from SSA unless the EIEP's client system contains a record of the subject individual's SSN. A properly configured Permission Module also enforces referential integrity and prevents unauthorized random browsing of PII.

Screen Scraping:

Screen scraping is normally associated with the programmatic collection of visual data from a source. Originally, screen scraping referred to the practice of reading text data from a computer display terminal's screen. This involves reading the terminal's memory through its auxiliary port, or by connecting the terminal output port of one computer system to an input port on another. The term screen scraping is synonymous with the term bidirectional exchange of data.

A screen scraper might connect to a legacy system via Telnet, emulate the keystrokes needed to navigate the legacy user interface, process the resulting display output, extract the desired data, and pass it on to a modern system.

More modern screen scraping techniques include capturing the bitmap data from a screen and running it through an optical character reader engine, or in the case of graphical user interface applications, querying the graphical controls by programmatically obtaining references to their underlying programming objects.

Security Breach:

An act from outside an organization that bypasses or violates security policies, practices, or procedures.

Security Incident:

A security incident happens when a fact or event signifies the possibility that a breach of security may be taking place, or may have taken place. All threats are security incidents, but not all security incidents are threats.

Security Violation:

An act from within an organization that bypasses or disobeys security policies, practices, or procedures.

Sensitive data:

Sensitive data is a special category of personally identifiable information (PII) that has the potential to cause great harm to an individual, government agency, or program if abused, misused, or breached. It is sensitive information protected against unwarranted disclosure and carries specific criminal and civil penalties for an individual convicted of unauthorized access, disclosure, or misuse. Protection of sensitive information usually involves specific classification or legal precedents that provide special protection for legal and ethical reasons.

Security Information Management (SIM):

SIM is software that automates the collection of event log data from security devices such as firewalls, proxy servers, intrusion detection systems and anti-virus software. The SIM translates the data into correlated and simplified formats.

SMDS (Switched Multimegabit Data Service (SMDS):

SMDS is a telecommunications service that provides connectionless, high-performance, packet-switched data transport. Although not a protocol, it supports standard protocols and communications interfaces using current technology.

SSA-provided data/information:

Synonymous with "SSA-supplied data/information", defines information under the control of SSA provided to an external entity under the terms of an information exchange agreement with SSA. The following are examples of SSA-provided data/information:

- SSA's response to a request from an EIEP for information from SSA (e.g., date of death)
- SSA's response to a query from an EIEP for verification of an SSN

SSA data/information:

This term, sometimes used interchangeably with "SSA-provided data/information," denotes information under the control of SSA provided to an external entity under the terms of an information exchange agreement with SSA. However, "**SSA data/information**" also includes information provided to the EIEP by a source other than SSA, but which the EIEP attests to that SSA verified it, or the EIEP couples the information with data from SSA as to certify the accuracy of the information. The following are examples of SSA information:

- SSA's response to a request from an EIEP for information from SSA (e.g., date of death)
- SSA's response to a query from an EIEP for verification of an SSN

- Display by the EIEP of SSA's response to a query for verification of an SSN *and* the associated SSN provided by SSA
- Display by the EIEP of SSA's response to a query for verification of an SSN *and* the associated SSN provided to the EIEP by a source other than SSA
- Electronic records that contain only SSA's response to a query for verification of an SSN *and* the associated SSN whether provided to the EIEP by SSA or a source other than SSA

SSN:

Social Security Number

STC:

A State Transmission/Transfer Component is an organization, which performs as an electronic information conduit or collection point for one or more other entities (also referred to as a hub).

System-generated transaction:

A transaction automatically triggered by an automated system process.

Example: A user enters a client's information including the client's SSN on an input screen and presses the "ENTER" key to acknowledge that input of data is complete. An automated process then matches the SSN against the organization's database and when the systems finds no match, automatically sends an electronic request for verification of the SSN to SSA.

Systems process:

Systems Process refers to a software program module that runs in the background within an automated batch, online, or other process.

Third Party:

Third Party pertains to an entity (person or organization) provided access to SSA-provided information by an EIEP or other SSA business partner for which one or more of the following apply:

- is not stipulated access to SSA-provided information by an information-sharing agreement between an EIEP and SSA
- has no data exchange agreement with SSA
- SSA does not directly authorize access to SSA-provided information

Transaction-driven:

This term pertains to an automatically initiated online query of or request for SSA information by an automated transaction process (e.g., driver license issuance, etc.). The query or request will only occur the automated process meets prescribed conditions.

Uncontrolled transaction:

This term pertains to a transaction that falls outside a permission module. An uncontrolled transaction is not subject to a systematically enforced relationship between an authorized process or application and an existing client record.

8. Regulatory References

- Federal Information Processing Standards (FIPS) Publications
- Federal Information Security Management Act of 2002 (FISMA)
- Homeland Security Presidential Directive (HSPD-12)
- National Institute of Standards and Technology (NIST) Special Publications
- Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*
- Office of Management and Budget (OMB) Circular A-130, Appendix III, *Management of Federal Information Resources*
- Office of Management and Budget (OMB) Memo M-06-16, *Protection of Sensitive Agency Information, June 23, 2006*
- Office of Management and Budget (OMB) Memo M-07-16, *Memorandum for the Heads of Executive Departments and Agencies May 22, 2007*
- Office of Management and Budget (OMB) Memo M-07-17, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007*
- Privacy Act of 1974, as amended

9. Frequently Asked Questions (Click links for answers or additional information)

1. Q: What is a [breach](#) of data?
A: Refer to [Security Breach](#), [Security Incident](#), and [Security Violation](#).
2. Q: What is employee [browsing](#)?
A: Requests for or queries of SSA-provided information for purposes not related to the performance of official job duties
3. Q: Okay, so the EIEP submitted the SDP. Can SSA schedule the Onsite

Review?

A: Refer to [Scheduling the Onsite Review](#).

4. Q: What is a “**Permission Module**?”

A: A utility or subprogram within an application, which automatically enforces the relationship of a request for or query of SSA-provided information to an authorized process or transaction before initiating a transaction. For example, if requests for verification of an SSN for issuance of a driver’s license happens automatically from within a state driver’s license application. The System will not allow a user to request information from SSA unless the EIEP’s client system contains a record of the subject individual’s SSN.

5. Q: What “**Screen Scraping**?”

A: Screen scraping is normally associated with the programmatic collection of visual data from a source. Originally, screen scraping referred to the practice of reading text data from a computer display terminal’s screen. This involves reading the terminal’s memory through its auxiliary port, or by connecting the terminal output port of one computer system to an input port on another. The term screen scraping is synonymous with the term bidirectional exchange of data.

A screen scraper might connect to a legacy system via Telnet, emulate the keystrokes needed to navigate the legacy user interface, process the resulting display output, extract the desired data, and pass it on to a modern system.

More modern screen scraping techniques include capturing the bitmap data from a screen and running it through an optical character reader engine, or in the case of graphical user interface applications, querying the graphical controls by programmatically obtaining references to their underlying programming objects.

6. Q: When does an EIEP have to submit an SDP?

A: Refer to [When the SDP is Required](#).

7. Q: Does an EIEP have to submit an SDP when the agreement is renewed?

A: The EIEP does not have to submit an SDP *because* the agreement between the EIEP and SSA was renewed. There are, however, circumstances that require an EIEP to submit an SDP.

Refer to [When the SDP is Required](#).

8. Q: Is it acceptable to save SSA-provided information with a verified indicator on a (EIEP) workstation if the EIEP uses an encrypted hard drive? If not, what options does the agency have?

A: There is no problem with an EIEP saving SSA-provided information on the encrypted hard drives of computers used to process SSA-provided information if the EIEP retains the information only as provided for in

the EIEP's data-sharing agreement with SSA.
Refer to [Data and Communications Security](#).

9. Q: Does SSA allow EIEPs to use caching of SSA-provided information on the EIEP's workstations?
A: Caching during processing is not a problem. However, SSA-provided information must clear from the cache when the user exits the application. Refer to [Data and Communications Security](#).
10. Q: What does the term "interconnections to other systems" mean?
A: As used in SSA's system security requirements document, the term "interconnections" is the same as the term "connections."
11. Q: Is it acceptable to submit the SDP as a .PDF file?
A: No, it is not. The document must remain editable.
12. Q: Should the EIEP write the SDP from the standpoint of the EIEP SVES (or applicable data element) access itself, or from the standpoint of access to all data provided to the EIEP by SSA?
A: The SDP is to encompass the EIEP's entire electronic access to SSA-provided information as per the electronic data exchange agreement between the EIEP and SSA.
Refer to [Developing the SDP](#).
13. Q: If the EIEP has a "transaction-driven" system, does the EIEP still need a permission module? If employees cannot initiate a query to SSA, why would the EIEP need the permission module?
A: "Transaction driven" means that queries submit requests automatically (and it might depend on the transaction). Depending on the system's design, queries might not be automatic or it may still permit manual transactions. A system may require manual transactions to correct an error. SSA does not prohibit manual transactions if an ATS properly tracks such transactions. If a "transaction-driven" system permits any type of alternate access, it still requires a permission module, even if it restricts users from performing manual transactions. If the system does *not* require the user to be in a particular application and/or the query to be for an existing record in the EIEP's system *before* the system will allow a query to go through to SSA, it would still need a permission module.
14. Q: What is an Onsite Compliance Review?
A: The Onsite Compliance Review is SSA's periodic site visits to its Electronic Information Exchange Partners (EIEP) to certify whether the EIEP's management, operational, and technical security measures for protecting data obtained electronically from SSA continue to conform to the terms of the EIEP's data sharing agreements with SSA and SSA's associated system security requirements and procedures.
Refer to the [Compliance Review Program and Process](#).

15. Q: What are the criteria for performing an Onsite Compliance Review?
A: The following are criteria for performing the Onsite Compliance Review:
- EIEP initiating new access or new access method for obtaining information from SSA
 - EIEP's cyclical review (previous review was performed remotely)
 - EIEP has made significant change(s) in its operating or security platform involving SSA-provided information
 - EIEP experienced a breach of SSA-provided personally identifying information (PII)
 - EIEP has been determined to be high-risk
16. Q: What is a Remote Compliance Review?
A: The Remote Compliance Review is when SSA conducts the meetings remotely (e.g., via conference calls). SSA schedules conference calls with its EIEPs to determine whether the EIEPs technical, managerial, and operational security measures for protecting data obtained electronically from SSA continue to conform to the terms of the EIEP's data sharing agreements with SSA and SSA's associated system security requirements and procedures. Refer to the [Compliance Review Program and Process](#).
17. Q: What are the criteria for performing a Remote Compliance Review?
A: The EIEP must satisfy the following criteria to qualify for a Remote Compliance Review:
- EIEP's cyclical review (SSA's previous review yielded no findings or the EIEP satisfactorily resolved cited findings)
 - EIEP has made no significant change(s) in its operating or security platform involving SSA-provided information
 - EIEP has not experienced a breach of SSA-provided personally identifying information (PII) since its previous compliance review.
 - SSA rates the EIEP as a low-risk agency or state

ATTACHMENT 5

SYSTEM CERTIFICATION REQUIREMENTS FOR THE CMS HUB

Not Applicable

Security Certification Requirements for use of the SSA Data Set via the Centers for Medicare & Medicaid Services' (CMS) Hub

The Social Security Administration (SSA) does not allow new data exchange partners to begin receiving data electronically until the Authorized State Agency submits an approved Security Design Plan (SDP). SSA's Office of Information Security (OIS) usually performs an onsite security review to verify and validate that the management, operational, and technical controls conform to the requirements of the signed agreements between SSA and the Authorized State Agency, as well as applicable Federal law and SSA's technical systems security requirements (Attachment 4 to the Information Exchange Agreement (IEA)). As it concerns the use of the *SSA Data Set* via the Hub, OIS will waive the initial SDP/Certification for an existing Authorized State Agency if it meets all the following criteria:

1. The Authorized State Agency already has a functioning CMS-approved Integrated Eligibility Verification System (IEVS).
2. The Authorized State Agency is already receiving data from the Hub to support the Medicaid program and/or the Children's Health Insurance Program (CHIP).
3. The Authorized State Agency will only process requests for the *SSA Data Set* for administration of health or income maintenance programs approved by SSA through the Hub in conjunction with Insurance Affordability Programs eligibility determinations.
4. The Authorized State Agency agrees that the SSA security controls identified in the IEA and Attachment 4 to the IEA will prevail for all SSA data received by the State Agency, including the *SSA Data Set*.
5. The Authorized State Agency agrees that a significant vulnerability or risk in a security control, a data loss, or a security breach may result in a suspension or termination of the *SSA Data Set* through the Hub. In this case, at SSA's request, the Authorized State Agency agrees to immediately cease using the *SSA Data Set* for all SSA authorized health or income maintenance programs until the State Agency sufficiently mitigates or eliminates such risk(s) and/or vulnerabilities to SSA's data.
6. The Authorized State Agency agrees not to process verification requests through the Hub from a standalone application for health or income maintenance program requests that have no connection to Insurance Affordability Programs eligibility determinations.

In the event that an Authorized State Agency decides to implement a new integrated eligibility system or use a different Authorized State Agency to implement the health or income maintenance data exchange process through the Hub, the Authorized State Agency will submit to SSA's OIS an SDP and be approved/certified prior to receipt of the *SSA Data Set* through the Hub. The Authorized State Agency will adhere to the following criteria, in addition to those stated in the IEA, section C, Program Questionnaire:

1. The Authorized State Agency agrees to provide an attestation to SSA that it has received certification through the CMS Hub approval MARS-E process.
2. The Authorized State Agency attests that it operates and has a CMS-approved IEVS and the IEVS initiates the request for the *SSA Data Set* for the State Agency's administration of health or income maintenance programs approved by SSA through the Hub in conjunction with Insurance Affordability Programs eligibility determinations.



3. The Authorized State Agency uses a streamlined multi-benefit application. The Authorized State Agency agrees not to process verification requests through the Hub from a standalone application for health or income maintenance program requests that have no connection to Insurance Affordability Programs eligibility determinations.
4. The Authorized State Agency will not request the *SSA Data Set* through the Hub until it has successfully begun using the Hub for administration of Insurance Affordability Programs eligibility determinations. SSA will begin sending the *SSA Data Set* to the Authorized State Agency after the State Agency verifies that the Hub process works, as required by the CMS Hub approval MARS-E process.
5. The Authorized State Agency agrees to participate in SSA's SDP/Certification process prior to transmitting requests for the *SSA Data Set* through the Hub and to participate in SSA's triennial security compliance reviews on an ongoing basis.
6. The Authorized State Agency agrees that a significant vulnerability or risk in a security control, a data loss, or a security breach may result in a suspension or termination of the *SSA Data Set* through Hub. In this case, at SSA's request, the Authorized State Agency agrees to immediately cease using the *SSA Data Set* for all SSA authorized health or income maintenance programs until the State Agency sufficiently mitigates or eliminates such risk(s) and/or vulnerabilities to SSA's data.



ATTACHMENT 6

**WORKSHEET FOR REPORTING LOSS OR PORTENTIAL LOSS
OF PERSONALLY INDETIFIABLE INFORMATION**

09/27/06

Worksheet for Reporting Loss or Potential Loss of Personally Identifiable Information

1. Information about the individual making the report to the NCSC:

Name:			
Position:			
Deputy Commissioner Level Organization:			
Phone Numbers:			
Work:		Cell:	Home/Other:
E-mail Address:			
Check one of the following:			
Management Official	<input type="checkbox"/>	Security Officer	Non-Management <input type="checkbox"/>

2. Information about the data that was lost/stolen:

Describe what was lost or stolen (e.g., case file, MBR data):

Which element(s) of PII did the data contain?

Name	<input type="checkbox"/>	Bank Account Info	<input type="checkbox"/>
SSN	<input type="checkbox"/>	Medical/Health Information	<input type="checkbox"/>
Date of Birth	<input type="checkbox"/>	Benefit Payment Info	<input type="checkbox"/>
Place of Birth	<input type="checkbox"/>	Mother's Maiden Name	<input type="checkbox"/>
Address	<input type="checkbox"/>	Other (describe):	<input type="checkbox"/>

Estimated volume of records involved:

3. How was the data physically stored, packaged and/or contained?

Paper or Electronic? (circle one):

If Electronic, what type of device?

Laptop	<input type="checkbox"/>	Tablet	<input type="checkbox"/>	Backup Tape	<input type="checkbox"/>	Blackberry	<input type="checkbox"/>
Workstation	<input type="checkbox"/>	Server	<input type="checkbox"/>	CD/DVD	<input type="checkbox"/>	Blackberry Phone #	<input type="checkbox"/>
Hard Drive	<input type="checkbox"/>	Floppy Disk	<input type="checkbox"/>	USB Drive	<input type="checkbox"/>		
Other (describe):							

09/27/06

Additional Questions if Electronic:

	Yes	No	Not Sure
a. Was the device encrypted?			
b. Was the device password protected?			
c. If a laptop or tablet, was a VPN SmartCard lost?			
Cardholder's Name:			
Cardholder's SSA logon PIN:			
Hardware Make/Model:			
Hardware Serial Number:			

Additional Questions if Paper:

	Yes	No	Not Sure
a. Was the information in a locked briefcase?			
b. Was the information in a locked cabinet or drawer?			
c. Was the information in a locked vehicle trunk?			
d. Was the information redacted?			
e. Other circumstances:			

4. If the employee/contractor who was in possession of the data or to whom the data was assigned is not the person making the report to the NCSC (as listed in #1), information about this employee/contractor:

Name:			
Position:			
Deputy Commissioner Level Organization:			
Phone Numbers:			
Work:	Cell:	Home/Other:	
E-mail Address:			

5. Circumstances of the loss:
- a. When was it lost/stolen?
 - b. Brief description of how the loss/theft occurred:
 - c. When was it reported to SSA management official (date and time)?
6. Have any other SSA components been contacted? If so, who? (Include deputy commissioner level, agency level, regional/associate level component names)

09/27/06

7. Which reports have been filed? (include FPS, local police, and SSA reports)

Report Filed	<u>Yes</u>	<u>No</u>	<u>Report Number</u>
Federal Protective Service			
Local Police			
	<u>Yes</u>	<u>No</u>	
SSA-3114 (Incident Alert)			
SSA-342 (Report of Survey)			
Other (describe)			

8. Other pertinent information (include actions under way, as well as any contacts with other agencies, law enforcement or the press):



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

For Clerk's Use Only:
AGENDA NUMBER

16

- Consent Departmental Correspondence Action Public Hearing
 Scheduled Time for Closed Session Informational

FROM: Health and Human Services – First 5

FOR THE BOARD MEETING: December 19, 2017

SUBJECT: Approval of amendment to the Children and Families Commission bylaws adding language that would allow the Board to appoint one alternate Board of Supervisor member to the First 5 Children and Families Commission

DEPARTMENTAL RECOMMENDATION:

Request Board: A) Approve amended bylaws* for the First 5 Children and Families Commission adding an alternate member of the Board of Supervisors to its composition; and either B) appoint from your membership an alternate member to the First 5 Children and Families Commission to fill the 2017 calendar year alternate position for the remainder of 2017; or C) choose to delay the alternate appointment until your board appoints 2018 commission members and alternates.

* The amended section of the Bylaws, if approved, will read as follows:

Article V: Membership

1. The Commission shall consist of seven members. Composition of the Commission shall be as follows:
 - a. One member and one alternate member shall be a member of the Board of Supervisors. The alternate member shall be entitled to vote in the absence of the Board of Supervisor member.

SUMMARY DISCUSSION:

At your January 17, 2017 meeting, staff provided background research regarding adding a Board of Supervisors alternate for various commissions. At the February 14, 2017 meeting, the Board further discussed adding alternates to certain boards and commissions on which Board members currently serve, and directed staff to introduce the idea of amending bylaws to allow for alternates to other commissions and return to the Board with feedback.

At the September 26, 2017 meeting, the Board introduced and waived further reading of the proposed ordinance to adopt Inyo County Ordinance which would amend Section 2.50.60 and add language to allow the Board to appoint one alternate Board of Supervisors member to the First 5 Children and Families Commission; on October 10, 2017, your Board adopted said Ordinance No. 1209 (attached).


On October 30, 2017, the First 5 Children and Families Commission took action to amend its bylaws in accordance with the new ordinance. Your Board is now being asked to approve the changes to the bylaws (attached) and, if it desires, appoint an alternate from among its membership to the First 5 Children and Families Commission. When presenting the possibility of alternates in January 2017, Chairperson Tillemans originally recommended Supervisor Griffiths as the alternate member for the First 5 Children and Families Commission. The Chairperson serves as the Board's primary representative on the Commission.

ALTERNATIVES:

Your Board could choose not to approve the amended Bylaws; this is not recommended as the Board then could not appoint an alternate Board of Supervisor member. Your Board could choose to appoint a different alternate than originally recommended, or elect to not appoint an alternate at this time.

OTHER AGENCY INVOLVEMENT: County Counsel, Clerk of the Board, First 5 Children and Families Commission

FINANCING: Outside of the staff time spent researching statute and bylaws, and the cost of public notice publications, there is no fiscal impact associated with this action.

<u>APPROVALS</u>	
COUNTY COUNSEL: 	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS (Must be reviewed and approved by county counsel prior to submission to the board clerk.) Approved: <u>YES</u> Date <u>12/5/17</u>
AUDITOR/CONTROLLER: N/A	ACCOUNTING/FINANCE AND RELATED ITEMS (Must be reviewed and approved by the auditor-controller prior to submission to the board clerk.) Approved: _____ Date _____
PERSONNEL DIRECTOR: N/A	PERSONNEL AND RELATED ITEMS (Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.) Approved: _____ Date _____

DEPARTMENT HEAD SIGNATURE: Marilyn Marm by Jody Veech Date: 12/7/17
(Not to be signed until all approvals are received)
(The Original plus 20 copies of this document are required)

ORDINANCE NO. 1209

AN ORDINANCE OF THE BOARD OF SUPERVISORS OF THE COUNTY OF INYO, STATE OF CALIFORNIA, AMENDING SECTION 2.50.060 OF THE INYO COUNTY CODE, PERTAINING TO THE MEMBERSHIP OF THE CHILDREN AND FAMILIES COMMISSION

WHEREAS, Section 2.50.060 of the Inyo County Code specifies the Commission shall consist of seven members; and

WHEREAS, the membership of the Commission currently consists of one member of the Board of Supervisors and six other members; and

WHEREAS, the Board wishes to amend Section 2.50.060 so that Board may appoint an alternate member for the one Board of Supervisor member;

NOW, THEREFORE, the Board of Supervisors of the County of Inyo ordains as follows:

SECTION I: Section 2.50.060 of the Inyo County Code is hereby amended in its entirety to read as follows:

“2.50.060 Membership.

The Commission shall consist of seven members. The membership shall consist of one member of the Board of Supervisors, and one alternate member of the Board of Supervisors, the health and human services department director or his/her designee, one designee of the health and human services director from persons listed at Health & Safety Code Section 130140 (a)(1)(A)(i), and four members who represent any of the following categories: (a) recipients of project services included in the county strategic plan; (b) educators specializing in early childhood development; (c) representatives of a local child care resource or referral agency, or a local child care coordinating group; (d) representatives of a local organization for prevention or early intervention for families at risk; (e) representatives of community-based organizations that have the goal of promoting nurturing and early childhood development; (f) representatives of local school districts; and (g) representatives of local medical, pediatric, or obstetric associations or societies.”

SECTION II: EFFECTIVE DATE

This Ordinance shall take effect and be in full force and effect thirty (30) days after its adoption. Before the expiration of fifteen (15) days from the adoption hereof, this Ordinance shall be published as required by Government Code Section 25124. The Clerk of the Board is hereby instructed and ordered to so publish this Ordinance together with the names of the Board members voting for and against same.

PASSED AND ADOPTED THIS 10th DAY OF October, 2017.

AYES: -5- Supervisors Griffiths, Kingsley, Pucci, Tillemans, Totheroh

NOES: -0-

ABSTAIN: -0-

ABSENT: -0-



**Mark Tillemans, Chairperson
Inyo County Board of Supervisors**

ATTEST:

**Kevin Carunchio
Clerk of the Board**

By: _____



Darcy Ellis, Assistant



**Inyo County Children and Families
Commission Bylaws**

Article I: Name

Inyo County Children and Families Commission

Article II: Authority

The Commission was created by the Inyo County Board of Supervisors pursuant to California health and Safety Code section 120110 et seq. ("Children and Families First Act of 1998"; hereafter "the Act".) The Inyo County Children and Families Commission is an agency of the county with independent authority over the strategic plan described in Health and Safety Code Section and the Inyo County Children and Family Trust Fund established pursuant to subparagraph (A) of paragraph (2) of subdivision(d) of Health & Safety code Section 130105.

Article III: Mission Statement

Recognizing that current research in brain development of young children indicated that the emotional, physical and intellectual environment in which a child grows up is critical to that child's development, the Inyo County Children and Families Commission is committed to building communities that support and insure healthy children, strong families and children learning and ready for school.

Article IV: Duties and Responsibilities

Under the general direction and approval of the Board of Supervisors the Inyo County Children and Families Commission shall:

1. Adopt an adequate and complete county strategic plan for the support and improvement of early childhood development with the county, consistent with the requirements of the Act and any state regulations or guidelines hereinafter enacted to implement the Act. The Commission shall conduct at least one public hearing on its proposed strategic plan before the plan is adopted.
2. Conduct at least one public hearing on its periodic review of the county strategic plan to measure outcomes of its funded programs through the use of reliable indicators before any necessary revisions to the plan are adopted.
3. Submit it's adopted county strategic plan and any subsequent revisions thereto, to the First 5 California Children and Families Commission and the Board of Supervisors.

4. Prepare and adopt an annual audit and report pursuant to Section 130150 of the Health and Safety Code Section 130150. The commission shall conduct at least one public hearing prior to adopting any annual audit report.
5. Conduct at least one public hearing on each annual report by the State Children and Families Commission prepared pursuant to Health and Safety Code Section 130150. The commission shall conduct at least one public hearing prior to adopting any annual audit report.
6. Make copies of its annual audits and reports available to members of the general public on request and at no cost.
7. Administer the moneys in the Children and Families Trust Fund, consistent with the requirements of the Act and its adopted strategic plan.
8. Prepare and adopt an annual budget for the administration and implementation of the Commission's Strategic Plan.
9. Apply for gifts, grants, donations, or contributions of money, property, facilities, or services from any person, corporation, foundation, or other public or private entity, in furtherance of a program of early childhood development.
10. Enter into such contracts as necessary or appropriated to carry out the provisions and purposes of this act.
11. To exercise all powers, duties, and functions as are prescribed by statute, the Board of Supervisors, and the Commission.

Article V: Membership

1. The Commission shall consist of 7 members. Composition of the commission shall be as follows:
 - a. One member and one alternate shall be a member of the Board of Supervisors. The alternate member shall be entitled to vote in the absence of the Board of Supervisor member.
 - b. One member shall be the Health and Human Services Director of his/her designee.
 - c. One member shall be designee, as defined in Health & Safety Code Section 130140, of the Health and Human Services Director.
 - d. Four members shall represent any of the following categories: recipients of project services included in the county strategic plan, educators specializing in early childhood development; representatives of a local childcare resource or referral agency, or a local child care coordination group; representative of a local organization for prevention or early intervention for families at risk; representatives of community-based organizations that have a goal of promoting, nurturing and early childhood development;

representatives of local school districts; and representatives of local medical, pediatric or obstetric association of societies.

2. Commission members shall be appointed by the Board of Supervisors. Commission members shall serve at the pleasure of the Board of Supervisors. The term of office of each member shall be for three years, and until the appointment of his/her successor.
3. Terms of office of the commission members shall be staggered. At the First meeting of the Commission, those two members representing various categories provided for in Section 2.59.060 shall classify themselves by lot so that one member shall have a term of office for three years, and the other member shall have a term of office for two years.
4. Notice of vacancies shall be shared with the community and the position shall be appointed by the Board of Supervisors. Efforts should be made to ensure that the racial and cultural composition of the Commission is reflective of persons and families within the community.
5. A vacancy on the Commission shall occur automatically on the occurrence of any of the following events before the expiration of the term:
 - a. Removal of the incumbent for any reason.
 - b. Death or resignation of the incumbent.
 - c. Ceasing to be a representative from the various categories provided for in Section 2.50.060 of the Inyo County Code. Failing to attend 75% of the Commission meetings within each twelve (12) month period.
6. The Board of Supervisors may remove a Commission member.
7. The Board of Supervisors shall make interim appointments to fill unexpired terms in the event of vacancies occurring during the term of members of the Commission. The Board of Supervisors shall act within sixty (60) days to fill a vacancy.
8. The Commission may appoint "non-voting" members to the Commission at its discretion. Non-voting members do not vote on formal actions taken by the Commission. Non-voting members shall be appointed, reappointed and/or removed.

Article VI: Officers and Duties

1. The officers of the Commission shall be a Chairperson, elected annually to serve for a term of one year, a Vice Chairperson and such officers as the Commission may designate. Pursuant to section 2.50.110 of the Inyo county Code, the commission shall make such rules and regulations as are necessary to conduct its business.
2. All officers shall be elected by a majority of the voting members of the Commission at a regular meeting or special meeting where a quorum is present. This person must be a member of the Commission duly appointed by the Board of Supervisors. All officers shall hold office

until their successors are duly elected. Officers may be re-elected to the same office or elected to a different office without restriction on the number of terms.

3. The Chairperson of the commission shall preside over all business and meetings of the commission. In the absence of the Chairperson, the Vice Chairperson shall conduct routine business matters and meetings.
4. The Health and Human Services Department Director, or his/her HHS designated commission member, shall serve as the liaison between the Commission and the Board of Supervisors and shall have the following duties:
 - a. The Commission Liaison shall certify the occurrence of any vacating event to the Board of Supervisors.
 - b. The Commission Liaison shall coordinate working operations between the Commission and necessary County offices regarding finances and operations, including appropriate oversight and administration of any contractual agreements for services as recommended by the Commission to the Board of Supervisors.
 - c. The Commission Liaison shall ensure the review of the Ordinance for continued appropriateness by the end of the first quarter of operation.

Article VII: Committees

1. The Commission shall establish one or more advisory committees to provide technical and professional expertise and support for purposes beneficial to accomplishing this Act.
2. Advisory committee members shall be paid reasonable per diem and reimbursement of reasonable expenses for attending meetings and discharging other official responsibilities inside and outside the County as authorized by the Commission, at the standard County rate.
3. To the extent feasible, the Commission shall utilize existing commissions, committees, and councils as technical advisory groups for purposes of strategic planning and program development.
4. Advisory Committees shall meet at the request of the Commission.

Article VIII: Meetings

1. The Commission shall meet as often as necessary to conduct business. The date, time, and place of meetings shall be established by majority vote of the Commission. The Commission's meetings are subject to the open meeting laws contained in the Ralph M. Brown Act.
2. A quorum shall be required for Commission actions. A quorum shall consist of a majority of the appointed members.

3. Approval of expenditure recommendations in excess of \$50,000, final adoption of the county strategic plan, and the election or removal of officers requires an affirmative vote of a majority of the members of the Commission.
4. Records shall be kept of all Commission actions as part of the Commission meeting minutes.

Article IX: Commission Work

The Commission shall retain authority to direct staff and assign duties as deemed necessary to conduct business.

Article X: Compensation

The members of the Commission shall serve without compensation, but may receive actual and necessary expenses as are incurred in carrying out their duties. This includes, but is not limited to, compensation for childcare for attendance of Commission meetings since our commission supports the importance of both quality child care services, and ensuring that parents from all walks of life are able to serve on our commission.

Article XI: Conflict of Interest

Commission members will declare to the Commission when they perceive a potential conflict of interest may be present, including but not limited to, situations involving financial interests of a member or a member's spouse, or with any agency or individual being considered for funding.

If any Commission member has a direct, indirect, or perceived conflict of interest with any decision being made by the Commission, the Commissioner shall declare the conflict and abstain from making, participating in making, or in any way attempting to use his or her official position to influence any decision by the Commission on any grant or contract. Such declaration of conflict and abstention shall be noted in the minutes.

Direct or indirect conflict of interest shall include, but not be limited to, the financial interests of a member or the member's spouse in any potential recipient (agency or individual) which is being considered for any grant or contract approved by the Commission.

All Commission members (voting and non-voting) shall abide by the Conflict of Interest Policies governing conflict of interest adopted by the Inyo County First Five Commission and applicable state law.

Article XII: Amendment of Bylaws

These Bylaws may be amended, with the exception of the rules of membership pursuant to section 2.50.060 of the county code, only by action of the Commission at any meeting of the

commission. Notice of such proposed amendment shall be given in the manner prescribed for notices of regular meetings of the Commission.

Reviewed and Approved by the Commission as is on	<u>October 30, 2017</u>		
Motion	<u>Lisa Fontana</u>	Seconded	<u>Robyn Wisdom</u>
Abstentions	<u>none</u>	Vote	<u>Ayes: 3 Noes: 0</u>



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

For Clerk's Use Only:
AGENDA NUMBER

17

- Consent Departmental Correspondence Action Public Hearing
 Scheduled Time for Closed Session Informational

FROM: Health and Human Services – First 5

FOR THE BOARD MEETING: December 19, 2017

SUBJECT: Appointment of members to five seats on the First 5 Children and Families Commission

DEPARTMENTAL RECOMMENDATION:

Request you Board appoint and/or reappoint the following individuals to the First 5 Children and Families Commission:

- Eileen Dougherty to an unexpired three-year term ending December 5, 2018 to be filled by a parent;
- Amanda Miloradich to an unexpired term ending December 5, 2018 to be filled by someone with experience in the early health field;
- Robyn Wisdom to a three-year term ending December 5, 2020 to be filled by a specialist in early childhood development;
- Melissa Best-Baker to an unexpired three-year term ending April 20, 2020 to be filled by the designee of the Health and Human Services Director, as defined in Health and Safety Code Section 130140; and
- Anna Scott to an unexpired three-year term ending April 20, 2020 to be filled by the Health and Human Services Director or his/her designee.

(Notices of Vacancy resulted in responses from the above-named individuals.)

SUMMARY DISCUSSION:

Your Board is asked to appoint and/or re-appoint five individuals to the First 5 Children and Families Commission whose terms either recently expired or who are seeking to be appointed to vacant seats. Five total positions were publicly advertised in October and November in accordance with County policy. Five responses were received by the application deadline of November 17, 2017. One application for the unexpired three-year term ending December 5, 2018 to be filled by a parent was received from Eileen Dougherty. One application for the unexpired term ending December 5, 2018 to be filled by someone with experience in the early health field was received from Amanda Miloradich. One application for the three-year term ending December 5, 2020 to be filled by a specialist in early childhood development was received from Robyn Wisdom. One application for the unexpired three-year term ending April 20, 2020 to be filled by the designee of the Health and Human Services Director was received from Melissa Best-Baker. One application for the unexpired three-year term ending April 20, 2020 to be filled by the Health and Human Services Director or his/her designee was received by HHS Director Marilyn Mann requesting Anna Scott's appointment.

ALTERNATIVES:

Your Board could choose to appoint or not reappoint different persons, other than those recommended, for the remaining Commission members; however, this is not recommended as these persons are qualified and the Commission needs to be fully staffed and finding other suitable members could take more time.

OTHER AGENCY INVOLVEMENT: County Counsel, Clerk of the Board, First 5 Children and Families Committee

FINANCING: Outside of the staff time spent researching statute and bylaws, and the cost of public notice publications, there is no fiscal impact associated with this action.

APPROVALS

COUNTY COUNSEL: <i>Neal Salter</i>	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS <i>(Must be reviewed and approved by county counsel prior to submission to the board clerk.)</i> Approved: <u><i>yes</i></u> Date <u><i>12/5/17</i></u>
AUDITOR/CONTROLLER:	ACCOUNTING/FINANCE AND RELATED ITEMS <i>(Must be reviewed and approved by the auditor-controller prior to submission to the board clerk.)</i> Approved: _____ Date _____
PERSONNEL DIRECTOR:	PERSONNEL AND RELATED ITEMS <i>(Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.)</i> Approved: _____ Date _____

DEPARTMENT HEAD SIGNATURE: *Marilyn Mann by Jody Velez* Date: *12/7/17*
(Not to be signed until all approvals are received)

RECEIVED

2017 NOV -7 AM 11:44

INYO COUNTY
ADMINISTRATOR
CLERK OF THE BOARD

August 24, 2017

Inyo County Board of Supervisors
224 N Edwards Street
Independence, CA 93526

Dear Inyo County Board of Supervisors,

I would love to rejoin the First 5 Inyo County Commission as a parent representative. My daughter Arrow Rose is now 1 year old and I've regained my energy for commission work. I believe in the mission of First 5 and my hope is that I can support its efforts. As a parent of small children I have experienced first hand the benefits of services First 5 has offered. I have taken multiple parenting classes and participated and conducted playgroups through First 5 Inyo and Mono Counties. I look forward to contributing and thank you for your consideration!

Sincerely yours,

Elleen Dougherty (Jackson)



Amanda Melissa Miloradich
3600 Ranch Road
Bishop, CA 93514
Home phone (760) 873-3466
Cellular (760) 937-6885
corgi@schat.net

November 10, 2017

Serena Johnson

First 5 Inyo County Director
County of Inyo
Health & Human Services Department
Drawer H, Independence CA, 93526
Telephone (760) 878-0247 or
163 May Street. Bishop, CA 93514
Telephone (760) 873-6505

RECEIVED
2017 NOV 15 PM 3:36
INYO COUNTY
ADMINISTRATOR
CLERK OF THE BOARD

Dear First 5 of Inyo County:

11/15/17

My name is Amanda Miloradich and I writing this letter in regards to becoming a volunteer health expert for the Inyo County First 5 Commission. Eileen Jackson, Inyo County First 5 Commissioner, nominated me for the volunteer position of the Inyo County First 5 Children and Families Commission. I am aware that that this position focus on young children 0-5 years old and their families. I have experience in early childhood health, education activities and services that include children's disabilities, nutrition and Mental Health. My experience stretches over 23 years of working for the Bishop Paiute Tribal Council. The following information will suggest why I feel that I would be a suitable candidate for the position of Inyo County First 5 Commissioner:

- I was employed at the Bishop Indian Education Center for 8 years as tutor, transportation service provider, Math, Science and Engineering Instructor, Hands on Science Outreach Instructor, children's meal services provider and a summer school activities teacher. I discontinued my employment at the Bishop Indian Education Center 2 weeks before my son was born.
- I began working at Bishop Indian Head Start preschool in 2002 as the Health/Disabilities Manager and Mental Health Coordinator. I substitute in the classrooms at Bishop Indian Head start when Teachers/Teacher's Assistants are unavailable. I am currently still employed at Bishop Indian Head Start Preschool. I have a California Teaching Permit as an Assistant Teacher. I will be furthering my education in January to hold a California Teacher's Permit.
- I have a Associates Degree in Liberal Arts specializing in Social and Behavioral Science from Truckee Meadows Community College and Cerro Coso Community College
- For 5 years I have been a Certified Child Passenger Safety Technician to be able to educate and install Car Seats. I am also an Inyo County Car Seat Coalition member.

Amanda Melissa Miloradich
3600 Ranch Road
Bishop, CA 93514
Home phone (760) 873-3466
Cellular (760) 937-6885
corgi@schat.net

- This is my second year as a CPR, First Aid, AED Instructor for the American Heart Association
- I have completed the Emergency Medical Technician (EMT) Course
- I have certificates of competition from the Department of Health and Human Services in Injury prevention I and II courses
- Certification has been completed so that I am able to conduct hearing and vision screenings with children
- I have written numerous grants that have been awarded to Bishop Indian Head Start in health and safety. The grants have included a health and nutrition First 5 mini grant, Department of Health and Human Services, IHS Ride Safe Car Seat grant, Sleep Safe Smoke Alarm grant and a California Department of Health, Child Plate's grant for Smoke Alarms. The Department of Health and Human Services IHS grants were awarded for the maximum time frame of five years consecutive at Bishop Indian Head Start.

I truly hope that you will consider me to hold a volunteer position on the Inyo County First 5 Commission. Thank you.

Sincerely,

Amanda Melissa Miloradich

Inyo County Board of Supervisors
PO Drawer N
Independence, CA 93526

RECEIVED
2017 NOV 14 PM 4: 22
INYO COUNTY
ADMINISTRATOR
CLERK OF THE BOARD

November 14, 2017

Honorable Board of Supervisors;

I am requesting reappointment to the Inyo County First 5 Commission. I currently serve in the position as Early Childhood specialist and my term will expire December 5, 2017. I enjoy serving on the Commission and would like to continue my service with First 5.

Thank you for considering this request for reappointment to the Inyo County First 5 Children and Families Commission.

Sincerely;



Robyn Wisdom
2168 Kiowa Circle
Bishop, CA 93514



County of Inyo

HEALTH & HUMAN SERVICES DEPARTMENT
Aging Services, Behavioral Health, Public Health, Social Services, First 5, Prevention

Drawer H, Independence, CA 93526
Telephone (760) 878-0247 FAX: (760) 878-0266

Or
163 May St., Bishop, CA 93514
Telephone (760) 873-3305 FAX: (760) 873-6505

MARILYN MANN, INTERIM DIRECTOR
mmann@inyocounty.us

November 8, 2017

Inyo County Board of Supervisors
P.O. Drawer N
Independence, CA 93526

Dear Supervisors:

I am requesting to be reappointed to the First 5 Inyo Children and Families First Commission as a designee of Health and Human Services for a three-year term ending April 20, 2020. I am the fiscal supervisor for all Health and Human Services funding and can use that information to provide guidance to the Commission on upcoming projects. In addition, I have worked with Jody Veenker and Serena Johnson to complete State reports and required outside audits.

Please contact me if you have any questions at 760-878-0232 or via email at mbestbaker@inyocounty.us.

Sincerely,

Melissa Best-Baker
Senior Management Analyst
760-878-0232
mbestbaker@inyocounty.us

RECEIVED
2017 NOV -9 AM 7:55
INYO COUNTY
ADMINISTRATOR
CLERK OF THE BOARD

County of Inyo

HEALTH & HUMAN SERVICES DEPARTMENT

*Behavioral Health, Public Health, Social Services, First 5, Prevention,
Aging Services*



*Drawer H, Independence, CA 93526
Telephone (760) 878-0247 FAX: (760) 878-0266*

Or

*163 May St., Bishop, CA 93514
Telephone (760) 873-3305 FAX: (760) 873-6505*

MARILYN MANN, DIRECTOR

mman@inyocounty.us

November 17, 2017

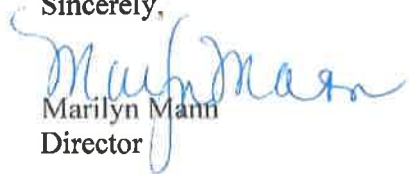
Inyo County Board of Supervisors
c/o Clerk of the Board
P.O. Drawer N
Independence, CA 93526

Honorable Board Members:

Inyo County Code requires that the Inyo County First 5 Children and Families Commission membership shall consist of the Health and Human Services Director or his/her designee. I would like to recommend that your Board appoint Anna Scott, HHS Deputy Director- Public Health and Prevention, as the Health and Human Services Director designee to the Commission. Ms. Scott currently provides management oversight to First 5, as it is housed in the Public Health and Prevention division. She will bring a high level of understanding and knowledge to the Commission, consulting with me as needed.

Thank you in advance for your consideration!

Sincerely,


Marilyn Mann
Director

Cc: Anna Scott
File



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

- Consent Departmental Correspondence Action Public Hearing
 Schedule time for _____ Closed Session Informational

For Clerk's Use
Only:

AGENDA NUMBER

18

FROM: Public Works Department

FOR THE BOARD MEETING OF: December 19, 2017

SUBJECT: Receive Report on Status of Independence Town Water System Transmission Main

DEPARTMENTAL RECOMMENDATIONS:

Request Board 1) receive report from staff on the status of the Independence Town Water System transmission main and 2) authorize staff to proceed with emergency repairs

CAO RECOMMENDATION:

SUMMARY DISCUSSION:

The Independence Town Water System transmission main has reached the end of its useful life. The transmission main conveys water from the wells to the storage tanks and also from the storage tank back into town to the distribution system. This pipe has been in place since 1928, was used pipe when installed, and it is estimated to have been in service in excess of 100 years. There are currently 5 leaks of various sizes in the main that we are attempting to control through the use of repair clamps. These efforts are of limited effectiveness due to the deteriorated, fragile condition of the pipe. To address the imminent failure of this pipe, staff has identified three separate actions which must undertaken.

1. Emergency plan in case of near term catastrophic failure.

This work has already been started. We are currently prepared to isolate and take the tanks off line and supply water directly from the wells. The down side of this is that the wells must be run constantly and a substantial amount of water would be wasted. Additionally, this will not supply water during a power outage without a generator. To most efficiently deal with this, Public Works will be renting a generator and transfer switch for approximately one month. The cost is estimated at \$15,000. These funds will be found within the Town Water System budgets. And, because the wells must be run constantly and water wasted, there is a likelihood that the water allotments specified in the Long Term Water Agreement for the Independence Town Water System will exceeded in which case the Town Water System may need to reimburse LADWP for water used in excess of the specified allotment.

2. Temporary emergency replacement of transmission main.

To avoid a catastrophic failure of the pipe, it recommended that a temporary 12" HDPE pipe be rented installed above ground to replace to existing line for an interim period. It is recommended that this work be accomplished in the next 30 days. Costs for this are:

- \$12,000 to install connection points on the existing line.
- \$21,000 for delivery, installation and the removal of the HDPE pipe.
- \$105,000 for pipe rental for up to 2 years. This is a monthly rental that can be stopped at any time.

3. Permanent replacement.

A permanent line needs to be installed to replace the existing main. We are estimating this cost to be about \$500,000. This could vary either up or down depending on the level of environmental analysis necessary, rights of way considerations, and determination of whether or not redundancy in the line is cost effective. These factors will also affect the time necessary to complete the permanent replacement.

Not coincidentally, a leak detection and condition assessment has been approved for completion for both the Independence and Lone Pine systems, by the California Rural Water Association in January. This will assist in our search for both grant and low interest loan funding for the permanent replacement.

Staff is recommending that the Board authorize installation of the temporary emergency transmission main.

ALTERNATIVES:

- 1) The Board could choose to not complete the interim improvement. This is not recommended as the line is failing and efforts to place multiple repair clamps have been unsuccessful due to the fragile condition of the deteriorated pipe. Having the interim line in will minimize financial as well as health and safety impacts to the Independence Town Water System.

OTHER AGENCY INVOLVEMENT:

-LADWP


FINANCING:

To the extent available, funds from the Town Water Systems budgets will be used to pay for costs associated with the temporary emergency replacement of transmission main, with budget amendments being brought before your Board as soon as practicable.

To the extent that funds do not or will not exist in the Water Systems funds to sustain the temporary or permanent solutions, your Board will need to consider other options which could include a County loan to this enterprise fund. This loan could be repaid in a number of ways including an emergency rate increase or as part of the normal rate evaluation already approved by your Board. These would, of course, need to meet all Proposition 218 requirements. As noted above, staff will also be pursuing grant funding for these repairs.

APPROVALS	
COUNTY COUNSEL:	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS (Must be reviewed and approved by County Counsel prior to submission to the board clerk.) Approved: _____ Date _____
AUDITOR/CONTROLLER	ACCOUNTING/FINANCE AND RELATED ITEMS (Must be reviewed and approved by the auditor/controller prior to submission to the board clerk.) Approved: _____ Date _____
PERSONNEL DIRECTOR	PERSONNEL AND RELATED ITEMS (Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.) Approved: _____ Date _____

DEPARTMENT HEAD SIGNATURE:
(Not to be signed until all approvals are received)

 Date: 12/14/17



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

- Consent Departmental Correspondence Action Public Hearing
 Schedule time for Closed Session Informational

For Clerk's Use Only: AGENDA NUMBER 19
--

FROM: Public Works Department

FOR THE BOARD MEETING OF: December 19, 2017

SUBJECT: Request for Budget Amendment to increase revenue and appropriations for the Bishop Airport Apron Project.

DEPARTMENTAL RECOMMENDATIONS:

Request Board amend the Fiscal Year 2017-2018 Bishop Airport Apron (630304) as follows: increase estimated revenue in Federal Grants (4555) by \$154,375 and increase appropriations in Professional Services (5265) by \$154,375. (4/5's vote required.)

CAO RECOMMENDATION:

SUMMARY DISCUSSION:

At the February 21, 2017 meeting of the Board of Supervisors, your Board approved Amendment 14 to the Contract with Wadell Engineering Corporation for On-Call Airport Engineering and Planning Services for the Bishop Airport Terminal Area Apron Rehabilitation Design in the amount of \$154,375.00. On August 15, 2017 the FAA funded the 90% of the project under AIP Grant Number 3-06-0024-019-2017 in the amount of \$1,671,931.00. The funded amount included costs for administrative fees, construction inspection and construction of the Apron. The design of the Apron was not included in this grant. Correspondence from FAA on August 18, 2017 stated that grant 3-06-0024-019-2017 can fund the design and any overage of the grant can be funded through the amendment process at the end of the project up to 15% of the grant amount which is \$250,789.65. The amendment to the Bishop Apron budget (630304) is to cover the costs of the design which was approved by the FAA to be expensed from grant 3-06-0024-019-2017.

ALTERNATIVES:


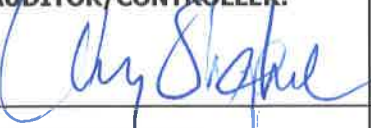

The Board could choose not to approve the budget amendment, however it is not recommended as the design services have already been provided.

OTHER AGENCY INVOLVEMENT:

FINANCING:

This budget amendment will be funded out of Bishop Apron budget (630304) which will be reimbursed at 100% Federal, object code 4555. This project has already been approved.

APPROVALS

COUNTY COUNSEL: 	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS <i>(Must be reviewed and approved by County Counsel prior to submission to the Board Clerk.)</i> Approved: <u>YES</u> Date: <u>12/6/17</u>
AUDITOR/CONTROLLER: 	ACCOUNTING/FINANCE AND RELATED ITEMS <i>(Must be reviewed and approved by the Auditor/Controller prior to submission to the Board Clerk.)</i> Approved: <u>YES</u> Date: <u>12/12/17</u>
BUDGET OFFICER: 	BUDGET RELATED ITEMS Approved: <u>✓</u> Date: <u>12-12-2017</u>

DEPARTMENT HEAD SIGNATURE:

(Not to be signed until all approvals are received)
(The Original plus 20 copies of this document are required)



Date: 12/12/17



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

- Consent Departmental Correspondence Action Public Hearing
- Schedule time for Closed Session Informational

For Clerk's Use Only:
AGENDA NUMBER
20

FROM: Public Works Department

FOR THE BOARD MEETING OF: December 19, 2017

SUBJECT: Approve Parking Agreement with Eastern Sierra Transit Authority, JPA and the County of Inyo

DEPARTMENTAL RECOMMENDATIONS:

1. Request your Board approve the Lease Agreement between the County of Inyo and Eastern Sierra Transit Authority, JPA for the parking space at the Bishop Airport, Bishop, Ca for an initial period of two years with four, one year options to extend, in an annual amount of Three Thousand Three Hundred Twelve Dollars (\$3,312) payable to the County in a monthly installments of Two Hundred Seventy Six Dollars (\$276) Beginning on December 1, 2017 and ending November 30, 2019.
2. Authorize the Chairperson to sign the Lease Agreement contingent upon the appropriate signatures being obtained and contingent upon the adoption of future budgets.

CAO RECOMMENDATION:

SUMMARY DISCUSSION:

This lease provides office space for Eastern Sierra Transit Authority, JPA located in Bishop Ca. The lease agreement provides for an initial term of two years, commencing on December 1, 2017 and ending November 30, 2019 with four, one year options to extend. The monthly lease for the initial term is Two Hundred Seventy Six Dollars (\$276) per month or Three Thousand Three Hundred Twelve Dollars (\$3,312) per year. Should the County exercise the option for the extensions the amount will increase by two point five percent (2.5%) per year. If your board approves this lease and the County exercises all four one-year options to extend the amount payable to the County will be Twenty One Thousand One Hundred Fifty Six Dollars (\$21,156).

ALTERNATIVES:

Your Board could deny this Lease Agreement. This is not recommended, as doing so would leave Eastern Sierra Transit Authority, JPA without parking space. No other parking space has been identified at this time.

OTHER AGENCY INVOLVEMENT:

County Counsel for review
Auditor for review and payments

FINANCING:

Financing for this lease payment will be the responsibility of Eastern Sierra Transit Authority, JPA but will credit Bishop Airport 150100 rents and leases 4311.

APPROVALS

COUNTY COUNSEL: AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS (Must be reviewed and approved by County Counsel prior to submission to the board clerk.)
Jan Walker Approved: YES Date 12/5/17

AUDITOR/CONTROLLER ACCOUNTING/FINANCE AND RELATED ITEMS (Must be reviewed and approved by the auditor/controller prior to submission to the board clerk.)
Jim Stept Approved: YES Date 12-8-17

PERSONNEL DIRECTOR PERSONNEL AND RELATED ITEMS (Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.)
Approved: _____ Date _____

DEPARTMENT HEAD SIGNATURE: *St. Williams* Date: 12/8/17
(Not to be signed until all approvals are received)

**COUNTY OF INYO – BISHOP AIRPORT
GROUND LEASE**

THIS LEASE AGREEMENT, made and entered into this _____ day of _____, by and between **Eastern Sierra Transit Authority, JPA**, hereinafter referred to as "Lessee," and the County of Inyo, a political subdivision of the State of California, hereinafter referred to as "County," whereby the parties hereto agree as follows:

WITNESSETH:

SECTION 1. ADMINISTRATION.

This Lease Agreement, hereinafter referred to as "Lease," shall be administered on behalf of the County by Shannon Williams, whose title is Deputy Public Works Director, hereinafter referred to as "County's Lease Administrator" and on behalf of Lessee by Lessee's Executive Director.

SECTION 2. LEASED PREMISES.

County hereby leases to Lessee the real property (hereinafter referred to as "Leased Premises") located at the Eastern Sierra Regional Airport (hereinafter referred to as "Airport"), County of Inyo, State of California, and described more particularly as:

A dedicated bus parking area consisting of approximately 39,086 square feet of area just south of the south entrance to the road to the airport terminal as shown on Exhibit "A" attached hereto.

SECTION 3. INITIAL TERM AND OPTIONS.

The initial term of the Lease will be for Two (2) years beginning December 1, 2017, and continuing through and including November 30, 2019. In addition to the initial term, there will be four (4) options to extend the Lease for additional one (1) year periods as follows:

- a. From December 1, 2019 through November 30, 2020.
- b. From December 1, 2020 through November 30, 2021.
- c. From December 1, 2021 through November 30, 2022.
- d. From December 1, 2022 through November 30, 2023.

The options to extend may be exercised in the manner and under the conditions hereinafter provided.

SECTION 4. EXERCISING OPTIONS TO EXTEND TERM.

The four (4) options to extend the term of the Lease for one (1) year periods identified in Section Three above, may be exercised by Lessee in the manner and on the terms and conditions below:

- a. Terms and Conditions.
- (1) Neither Lessee nor County has terminated this Lease, or any extensions thereof, for any reason.
 - (2) Lessee is not in default under any term or condition of the Lease, or any extension thereof.
 - (3) Lessee has exercised all previous options to extend.
- b. Manner In Which Option Can Be Exercised.
- (1) Lessee may exercise the option to extend no earlier than six (6) months before the expiration of the Lease term, or any extension thereof.
 - (2) Lessee must notify County in writing of the intent to exercise an option to extend at least thirty (30) days before the expiration of the Lease term, or an extension thereof.
 - (3) Except as provided for in Section Six relating to the rent, the Option to Extend shall be upon the same terms and conditions as stated in this Lease.

SECTION 5. HOLDING OVER.

If Lessee remains in possession of the Leased Premises with the consent of County, either expressed or implied, after the expiration of the Lease term, Lessee's tenancy shall be deemed to be a tenancy from month to month at the same rental rate applicable for the final month of the Lease term and otherwise shall be upon the same terms and conditions as are set forth in the Lease, provided that such tenancy shall be terminable and may be terminated upon at least thirty (30) days prior written notice of such termination served by either Lessee or County on the other party in the manner prescribed by law.

SECTION 6. LEASE PAYMENTS.

Lessee will pay to County an annual Lease payment of Three Thousand Three Hundred and Twelve Dollars (\$3,312.00). Lessee agrees to pay County said amount in installments of Two Hundred and Seventy Six Dollars (\$276.00) per month, beginning December 1, 2017, and payable on the first of each month thereafter during the term of this lease, or any extension thereof.

In the event the Lessee exercises its option to extend the Lease for any or all of the four one-year periods, the rent for such option period may increase as agreed upon between County and Lessee, but such increase shall not exceed two and a half percent (2.5%) of the rent for the previous lease period. In the event County and Lessee do not agree upon a rental amount, the rent shall increase by the aforementioned percentage.

Lease payments will be made without set off, and without regard to any claim of contribution, improvement, or counter claim.

If the Lease or any extension thereof is terminated before the expiration of the complete term, the annual lease payment due will be prorated for the actual term of the Lease, or any extension thereof.

SECTION 7. USE OF PREMISES.

The premises are leased to be used for parking fleet vehicles. Lessee agrees to restrict its use to such purposes, and not to use or permit the use of the premises for any other purpose without first obtaining the consent in writing of County.

SECTION 8. MASTER LEASE.

The property herein leased by County to Lessee is the subject of a master lease between County and the Department of Water and Power of the City of Los Angeles, Numbered BL 120, and by this reference incorporated into this Lease. This Lease by the County of Inyo is subject to all of the terms and conditions imposed upon County by said master lease, and Lessee hereunder hereby agrees to abide by all of the terms of said master lease.

SECTION 9. DELIVERY OF POSSESSION.

Delivery of possession shall be deemed completed as of the date of execution of this instrument. Lessee represents and warrants that Lessee has examined the Leased Premises.

SECTION 10. QUIET POSSESSION.

The County covenants and agrees that Lessee, upon payment of the annual Lease payment and compliance with all the terms and conditions of this Lease, may lawfully, peacefully, and quietly have, hold, use, occupy, and enjoy the leased premises and each part thereof during the term of this Lease and any extensions thereof without hindrance or interruption by County.

SECTION 11. PARKING.

Lessee shall have reasonable non-exclusive use of the Airport parking area in common with other tenants, occupants, and users of the Airport, together with the right of reasonable ingress and egress to the Airport parking area.

SECTION 12. HOURS OF USE.

Lessee shall have access to the leased premises at any time on a twenty-four hour per day, seven-day per week basis.

SECTION 13. UTILITIES.

All charges for utilities used by Lessee in connection with the occupancy of the leased premises, (including deposits, connection fees or charges, meter rentals required by the supplier of any such utility service, and the cost of the facilities for connecting the leased premises to such utility services facilities) shall be paid by Lessee.

SECTION 14. MAINTENANCE.

Lessee agrees to maintain the Leased premises and any improvements thereon in good condition as reasonably required by the County throughout the term of the Lease.

SECTION 15. ENTRY FOR INSPECTION AND MAINTENANCE.

County reserves the right to enter the leased premises at reasonable times, with twenty-four (24) hour prior notification to the Lessee, to inspect, to perform required maintenance and repair, or to make additions or alterations to any part of the premises. County also reserves the

right to enter the leased premises at any time without prior notice to the Lessee in the event that an emergency reasonably requires the County to do so. Lessee agrees to permit County to do so. County may, during such time as is reasonably necessary to either respond to an emergency or to make such alterations, additions, or repairs, erect scaffolding, fences, and similar structures, post relevant notices, and place movable equipment without any obligation to reduce Lessee's rent for the demised premises during such period, and without incurring liability to Lessee for disturbance of quiet enjoyment of the premises, or loss of occupation thereof.

SECTION 16. ALTERATIONS AND IMPROVEMENTS.

Lessee shall make no alternations or improvements in or on the Leased Premises without the prior written consent of County. All alterations and improvements made by Lessee shall be removed from the Leased Premises upon the expiration or sooner termination of the Lease, unless otherwise agreed in writing by Lessee and County. Any damage occasioned by the installation or removal of Lessee's improvements shall be repaired by Lessee.

SECTION 17. SIGNS.

Lessee may erect signs necessary to identify Lessee's occupancy of the leased premises during the term hereunder. Lessee shall not place the proposed signs on the leased premises until County has reviewed the proposed design and given its consent to the proposed signs. County shall not unreasonably withhold said consent. Signs shall be removed by Lessee at the termination of this Lease.

SECTION 18. WASTE.

Lessee shall give prompt notice to County of any damages to the leased premises and shall not commit, or suffer to be committed, any waste or injury, or allow any public or private nuisance on the leased premises.

SECTION 19. WORKERS' COMPENSATION.

Lessee shall provide Statutory California Worker's Compensation coverage and Employer's Liability coverage for not less than \$1,000,000 per occurrence for all employees engaged in services or operations under this Agreement. The County of Inyo, its agents, officers and employees shall be named as additional insured or a waiver of subrogation shall be provided.

SECTION 20. INSURANCE.

Lessee shall procure and maintain for the duration of the contract insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the work hereunder and the results of that work by the Lessee, his agents, representatives or employees.

- A. Minimum Scope of Insurance. Coverage shall be at least as broad as:
1. Insurance Services Office Commercial General Liability coverage (occurrence Form CG 0001).
 2. Insurance Services Office Form Number CA 0001 covering Automobile Liability, code 1 (any auto).
 3. Workers' Compensation insurance as required by the State of California and Employer's Liability Insurance.

4. Errors and Omissions liability insurance appropriate to the Lessee's profession. Architects' and engineers' coverage is to be endorsed to include contractual liability.

B. Minimum Limits of Insurance. Lessee shall maintain limits no less than:

1. General Liability (including operations, products and completed operations as applicable): \$1,000,000.00 per occurrence for bodily injury, personal injury and property damage. If Commercial General Liability insurance or other form with a general aggregate limit is used, either the general aggregate limit shall apply separately to this project/location or the general aggregate limit shall be twice the required occurrence limit.
2. Automobile Liability: \$300,000.00 per accident for bodily injury and property damage.
3. Employer's Liability: \$500,000.00 per accident for bodily injury or disease.
4. Errors and Omissions Liability: \$ n/a per occurrence.

C. Deductibles and Self-insured Retentions. Any deductibles or self-insured retentions must be declared to and approved by the County. At the option of the County, either the insurer shall reduce or eliminate such deductibles or self-insured retentions as respects the County, its officers, officials, employees and volunteers; or the Lessee shall provide a financial guarantee satisfactory to the County guaranteeing payment of losses and related investigations, claims administration, and defense expenses.

D. Other Insurance Provisions. The commercial general liability and automobile liability policies are to contain, or be endorsed to contain, the following provisions:

1. The County, its officers, officials, employees, and volunteers are to be covered as insureds with respect to liability arising out of automobiles owned, leased, hired or borrowed by or on behalf of the Lessee; and with respect to liability arising out of work or operations performed by or on behalf of the Lessee including materials, parts or equipment furnished in connection with such work or operations. General liability coverage can be provided in the form of an endorsement to the Lessee's insurance, or as a separate owner's policy (CG 20 10 11 85).
2. For any claims related to this project, the Lessee's insurance coverage shall be primary insurance as respects the County, its officers, officials, employees, and volunteers. Any insurance or self-insurance maintained by the County, its officers, officials, employees, or volunteers shall be excess of the Lessee's insurance and shall not contribute with it.
3. Each insurance policy required by this clause shall be endorsed to state that coverage shall not be canceled by either party, except after thirty (30) days prior written notice by certified mail, return receipt requested, has been given to the County.
4. Coverage shall not extend to any indemnity coverage for the active negligence of the additional insured in any case where an agreement to indemnify the additional insured would be invalid under Subdivision (b) of Section 2782 of the Civil Code.

E. Acceptability of Insurers. Insurance is to be placed with insurers with a current A.M. Best's rating of no less than A:VII. The County at its option may waive this requirement.

F. Verification of Coverage. Lessee shall furnish the County with original certificates and amendatory endorsements effecting coverage required by this clause. The endorsements should be on forms provided by the County or on other than the County's forms, provided those endorsements or policies conform to the requirements. All certificates and endorsements are to be received and approved by the County before work commences. The County reserves the right to require complete, certified copies of all required insurance policies, including endorsements effecting the coverage required by the specifications at any time.

SECTION 21. HOLD HARMLESS.

Lessee will defend, indemnify, and hold the County free and harmless from any and all costs, judgments, liability, damages, or expense, including costs of suit and attorney's fees, arising out of or from any claimed injury or damage to persons or property sustained in, on, or about the leased premises, or arising out of Lessee's operation of the leased premises, or as a result of Lessee's acts or omissions or those of Lessee's agents, officers, or employees, in carrying out any operation upon the airport property, or arising out of any condition in, on, or above, the leased property. Lessee specifically waives any and all claims against the County for damages or compensation claimed or sustained by reason of any defect, deficiency, or impairment of any water system, electrical supply system, or electrical apparatus or wiring services on leased property.

SECTION 22. COMPLIANCE WITH LAW.

Lessee shall, at its sole cost, comply with all requirements of all County, State and Federal ordinances, laws, rules, and regulations now in force, or which may hereafter be in force, pertaining to the use of leased premises, and shall faithfully observe and obey all County, State and Federal ordinances, laws, rules, and regulations now in force, or which hereafter may be in force. If Lessee's failure to obey and comply with any of these rules, laws, ordinances, or regulations results in any assessment of fines, penalty, or damages against the County, Lessee will pay such civil penalty, fines or assessments and any costs the County incurs in defending or adjudicating such violations.

SECTION 23. TAXES, ASSESSMENTS, AND FEES.

In accordance with Revenue and Taxation Code section 107.6, Lessee is hereby advised that this lease may create a possessory interest subject to property taxation and that, if such an interest is created, Lessee is solely responsible for the payment of all property taxes levied on that interest. In addition, Lessee shall timely pay all taxes and assessments of whatever character that may be levied or charged upon the leasehold estate in the Leased Premises, or upon Lessee's operations thereon. Lessee shall also pay all license or permit fees that may be necessary, or which may be required by law, for the conduct of its operations at the Leased Premises.

SECTION 24. GRANT AGREEMENT ASSURANCES.

The following assurances required by the Federal Government as a condition of the Grant Agreement for the Bishop Airport are hereby incorporated into, and made a condition of, this Lease:

- a. The Lessee, for himself, his heirs, personal representatives, successors in interest, and assigns, as a part of the consideration hereof, does hereby covenant and agree as a covenant running with the land that in the event facilities are constructed, maintained, or

otherwise operated on the said property described in this Lease for a purpose for which a DOT program or activity is extended or for another purpose involving the provision of similar services or benefits, the Lessee shall maintain and operate such facilities and services in compliance with all requirements imposed pursuant to Title 49, Code of Federal Regulations, DOT, Subtitle A, Office of the Secretary, Part 21, Nondiscrimination in Federally-Assisted Programs of the Department of Transportation-Effectuation of Title VI of the Civil Rights Act of 1964, and as said Regulations may be amended.

b. The Lessee, for himself, his personal representatives, successors in interest, and assigns, as a part of the consideration hereof, does hereby covenant and agree as a covenant running with the land that:

(1) No person on the grounds of race, color, or national origin shall be excluded from participation in, denied the benefits of, or be otherwise subjected to discrimination in the use of said facilities;

(2) That in the construction of any improvements on, over, or under such land and the furnishing of services thereon, no person on the grounds of race, color, or national origin shall be excluded from participation in, denied the benefits of, or otherwise be subject to discrimination;

(3) That the Lessee, licensee, permittee, etc. shall use the premises in compliance with all other requirements imposed by or pursuant to Title 49, Code of Federal Regulations, Department of Transportation, Subtitle A, Office of the Secretary, Part 21, Non-discrimination in Federally-Assisted Programs of the Department of Transportation-Effectuation of Title VI of the Civil Rights Acts of 1964, and as said Regulations may be amended.

c. In the event of a breach of any of the above nondiscrimination covenants, County shall have the right to terminate the Lease, and to re-enter and repossess said land and the facilities thereon, and hold the same as if said Lease had never been made or issued. This provision does not become effective until the procedures of 49 CFR Part 21 are followed and completed, including expiration of appeal rights.

d. Lessee shall furnish its accommodations and/or services on a fair, equal, and not unjustly discriminatory basis to all users thereof, and it shall charge fair, reasonable, and not unjustly discriminatory prices for each unit or services; provided that Lessee may be allowed to make reasonable and nondiscriminatory discounts, rebates, or other similar type of price reductions to volume purchasers.

e. Non-compliance with provisions of paragraph "d." above shall constitute a material breach hereof, and in the event of such non-compliance, the County shall have the right to terminate this Lease and the estate hereby created without liability therefore, or at the election of the County or the United States either or both said Governments shall have the right to judicially enforce those provisions.

f. Lessee agrees that it shall insert the above five provisions (paragraphs "a.", "b.", "c.", "d.", and "e.") in any lease, agreement, contract, or similar instrument, by which said Lessee grants a right or privilege to any person, firm, or corporation to render accommodations and/or services to the public on the premises herein leased.

g. Lessee assures that it will undertake an affirmative action program as required by 14 CFR Part 152, Subpart E, to insure that no person shall on the grounds of race, creed, color, national origin, or sex be excluded from participating in any employment activities covered in 14 CFR Part 152, Subpart E. Lessee assures that no person shall be excluded on these grounds from participating in or receiving the services or benefits of any program or activity covered by this subpart. Lessee assures that no person shall be excluded on these grounds from participating in or receiving the services or benefits of any program or activity covered by this subpart. Lessee assures that it will require that its covered sub-organizations provide assurances to Lessee that they similarly will undertake affirmative action programs and that they will require assurances from their sub-organizations, as required by 14 CFR 152, Subpart E, to the same effect.

h. County reserves the right to further develop or improve the landing area of the airport as it sees fit, regardless of the desires or view of Lessee, and without interference or hindrance.

i. County reserves the right to maintain and keep in repair all publicly owned facilities of the airport, together with the right to direct and control all activities of Lessee in this regard.

j. This Lease shall be subordinate to the provisions and requirements of any existing or future agreement between County and the United States relative to the development, operation, or maintenance of the airport.

k. There is hereby reserved to County, its successors and assigns, for the use and benefit of the public, a right of flight for the passage of aircraft in the airspace above the surface of the premises herein Leased. This public right of flight shall include the right to cause in said airspace any landing at, taking off from, or operation on the Airport.

l. Lessee agrees to comply with the notification and review requirements covered in Part 77 of the Federal Aviation Regulations in the event future construction of a building is planned for the Leased premises, or in the event of any planned modification or alteration of any present or future building or structure situated on the Leased premises.

m. Lessee, by accepting this Lease, expressly agrees for itself, its successors and assigns, that it will not erect or permit the erection of any structure or object, or permit the growth of any tree on the land leased hereunder, above the height set forth in Part 77 of Federal Aviation Regulations. In the event the aforesaid covenants are breached, County reserves the right to enter upon the land leased hereunder and to remove the offending structure or object or cut the offending tree, all of which shall be at the expense of Lessee.

n. Lessee, by accepting this Lease, agrees for itself, its successors and assigns, that it will not make use of the leased premises in any manner which might interfere with the landing and taking off of aircraft from the Airport, or otherwise constitute a hazard. In the event the aforesaid covenant is breached, County reserves the right to enter upon the premises hereby leased and cause the abatement of such interference at the expense of Lessee.

o. It is understood and agreed that nothing herein contained shall be construed to grant or authorize the granting of an exclusive right within the meaning of Section 308a of the Federal Aviation Act of 1958 (49 U.S.C. 1349a).

SECTION 25. MODIFICATION.

The terms and conditions of the Lease and any extension thereof may be modified, changed, or amended at any time only by the mutual written consent of Lessee and County.

SECTION 26. TERMINATION.

This Lease may be canceled and terminated by either party, without penalty, for any reason, at any time after execution of this Lease. Such cancellation and termination shall be effective on the sixtieth (60th) day after one party gives to the other written notice of termination. However, the giving of such notice shall not release either the County or the Lessee from full and faithful performance of all covenants of this Lease during the period between the giving of notice and the effective date of cancellation and termination.

SECTION 27. RETURN OF PROPERTY AT TERMINATION.

Lessee will return the property in good condition upon termination or expiration of the Lease.

SECTION 28. ASSIGNMENT AND SUBLEASE.

Lessee agrees not to assign this Lease or sublet the leased premises in part, or encumber its leasehold estate, or any interest therein, or permit the same to be occupied by another, either voluntarily or by operation of law, without first obtaining the written consent of County. Any such assignment or sublease shall not release Lessee from liability hereunder, and any assignee or sublessee shall expressly assume all Lessee's obligations hereunder. It is also agreed that the giving of a written consent required herein on any one or more occasions shall not thereafter operate as a waiver of the requirement for written consent on any one or more subsequent occasions.

SECTION 29. SUBORDINATION.

Lessee agrees that this Lease shall be subject and subordinate to any mortgage, trust deed, or like encumbrance heretofore or hereafter placed upon the leased premises by County, or its successors in interest, to secure the payment of monies loaned, interest thereon, and other obligations. Lessee agrees to execute and deliver, upon demand of County, any and all instruments desired by County subordinating in the manner requested by County this Lease to such mortgage, trust deed, or like encumbrance.

Notwithstanding such subordination, Lessee's right to quiet possession of the leased premises shall not be disturbed if Lessee is not in default and so long as Lessee shall pay the rent and observe and perform all of the provisions in this Lease, unless this Lease is otherwise terminated pursuant to its terms.

SECTION 30. MECHANICS LIEN.

Lessee agrees to keep the leased premises free from all mechanics' liens or other liens of like nature arising because of work done or materials furnished upon the leased premises at the instance of, or on behalf of Lessee, provided however that Lessee can contest such lien provided it post an adequate bond therefore.

SECTION 31. FORCE MAJEURE.

If either party hereto shall be delayed or prevented from their performance of any act required hereunder by acts of God, restrictive governmental laws or regulations, strikes, civil disorders, or other causes not involving the fault, and beyond the control, of the party obligated (financial inability excepted), performance of such act shall be waived for the period of the delay. However, nothing in this clause shall excuse the Lessee from the payment of any rental or other charge required of Lessee, except as may be expressly provided elsewhere in this Lease.

SECTION 32. WAIVER.

It is agreed that any waiver by Lessee of any breach of any one or more of the covenants, conditions, or terms of this Lease shall not be construed to be a waiver of any subsequent breach of the same or different provision of the Lease; nor shall any failure on the part of the Lessee to require exact, full, complete, and explicit compliance with any of the covenants or conditions of this Lease be construed as in any manner changing the terms hereof, nor shall the terms of this Lease be changed or altered in any way whatsoever other than by written amendment, signed by both parties.

SECTION 33. DEFAULT.

In the event that Lessee or County shall default in any term or condition of this Lease, and shall fail to cure such default within thirty (30) days following service upon the defaulting party of a written notice of such default specifying the default or defaults complained of, or if the default cannot reasonably be cured within thirty (30) days, the defaulting party fails to commence curing the default within thirty (30) days and thereafter to diligently and in good faith continue to cure the default, the complaining party may forthwith terminate this Lease by serving the defaulting party written notice of such termination.

SECTION 34. INUREMENT.

The Lease shall be binding upon and inure to the benefit of the parties hereto and their respective heirs, executors, administrators, legal representatives, successors, and assigns.

SECTION 35. SEVERABILITY.

If any provision of this Lease or the application thereof to any person or circumstances shall, to any extent, be invalid or unenforceable, the remainder of this Lease, or the application of such provisions to person or circumstances other than those as to which it is invalid or unenforceable, shall not be affected thereby, and each provision of this Lease shall be valid and be enforced to the fullest extent permitted by law.

SECTION 36. TIME IS OF ESSENCE.

Time is expressly declared to be of the essence in this Lease and in all of the covenants and conditions herein.

SECTION 37. ADDITIONAL TERMS AND CONDITIONS.

Additional terms and conditions of the Lease, if any, are set forth in the exhibits listed below, each of which is attached hereto and incorporated herein by this reference: Exhibit A, Exhibit B and Exhibit C.

SECTION 38. AMENDMENT.

The Lease may be amended only by a written document signed by all parties hereto.

SECTION 39. ENTIRE AGREEMENT.

The Lease contains the entire agreement between the parties hereto and supersedes all previous agreements between the parties with respect to the subject matter of the Lease.

SECTION 40. CONSTRUCTION OF AGREEMENT.

Both County and Lessee have had the opportunity to and have participated in the drafting and final preparation of this Lease agreement. For that reason, the Lease itself, or any ambiguity contain therein, shall not be construed against either the County or Lessee as the drafters of this document.

SECTION 41. NOTICE.

Any notice required by the Lease or applicable law to be given or served on Lessee or County may be given or served either by personal delivery to the County Lease Administrator or any one of the Lessees, by personal delivery to, or by depositing the notice in the United States Mail, postage prepaid, to the address of each party as given below:

COUNTY

Public Works Deputy Director
168 N. Edwards St., P.O. Drawer Q
Independence, CA 93526

**Department
Address
City and State**

LESSEE

Eastern Sierra Transit Authority
703 B Airport Road, P.O. Box 1357
Bishop, CA 93514

**Name
Address
City and State**

---o0o---

**COUNTY OF INYO - BISHOP AIRPORT
OFFICE AND COMMERCIAL SPACE LEASE**

Initial Term of Lease:
December 1, 2017 through November 30, 2019

IN WITNESS THEREOF, the parties hereto have set their hands and seals this _____
day of _____, 20_____.

COUNTY

LESSEE

Lease Administrator

By _____
Director, Department of Public Works

Signature

Type or Print Name

Date: _____

Date: _____

Approved as to form and legality:

County Counsel

Approved as to accounting form and content:

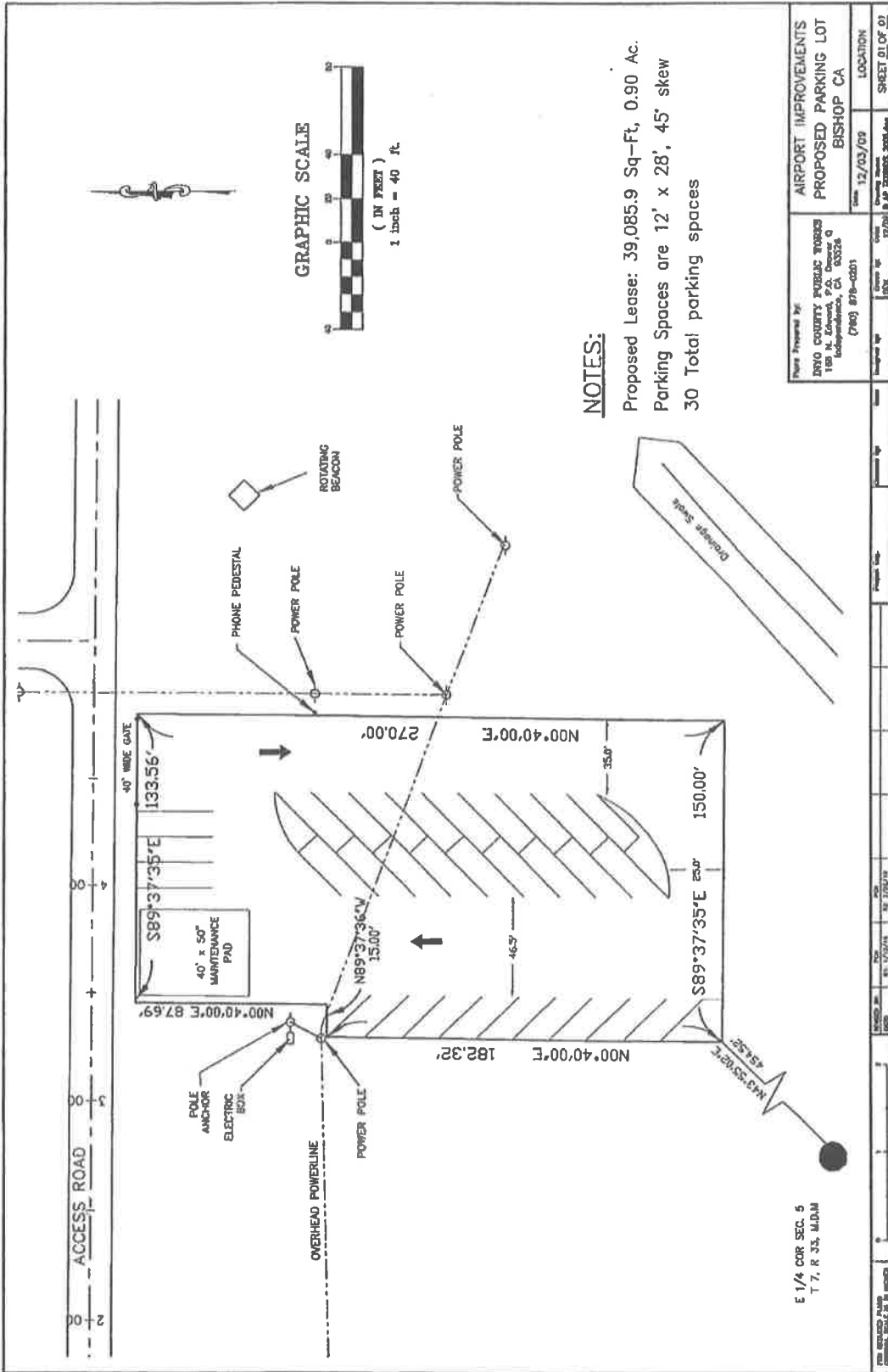
County Auditor

Approved as to insurance and risk management:

County Risk Manager

s:CountyCounsel/Leases

EXHIBIT A





AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

- Consent
 Departmental
 Correspondence Action
 Public Hearing
 Schedule time for
 Closed Session
 Informational

For Clerk's Use Only:
AGENDA NUMBER
21

FROM: Public Works Department

FOR THE BOARD MEETING OF: December 19, 2017

SUBJECT: Approve Office Lease Agreement with Eastern Sierra Transit Authority, JPA and the County of Inyo

DEPARTMENTAL RECOMMENDATIONS:

1. Request your Board approve the Lease Agreement between the County of Inyo and Eastern Sierra Transit Authority, JPA for the terminal building at the Bishop Airport, Bishop, Ca for an initial period of two years with four, one year options to extend, in an annual amount of Sixteen Thousand Five Hundred Sixty Dollars (\$16,560) payable to the County in a monthly installments of Thirteen Hundred Eighty Dollars (\$1380) Beginning on December 1, 2017 and ending November 30, 2019.
2. Authorize the Chairperson to sign the Lease Agreement contingent upon the appropriate signatures being obtained and contingent upon the adoption of future budgets.

CAO RECOMMENDATION:

SUMMARY DISCUSSION:

This lease provides office space for Eastern Sierra Transit Authority, JPA located in Bishop Ca. The lease agreement provides for an initial term of two years, commencing on December 1, 2017 and ending November 30, 2019 with four, one year options to extend. The monthly lease for the initial term is One Thousand Three Hundred Eighty Dollars (\$1380) per month or Sixteen Thousand Five Hundred Eighty Dollars (\$16,580) per year. Should the County exercise the option for the extensions the amount will increase by two point five percent (2.5%) per year. If your board approves this lease and the County exercises all four one-year options to extend the amount payable to the County will be One Hundred Five Thousand Seven Hundred Eighty One Dollars (\$105,781).

ALTERNATIVES:

Your Board could deny this Lease Agreement. This is not recommended, as doing so would leave Eastern Sierra Transit Authority, JPA without office space. No other office space has been identified at this time.

OTHER AGENCY INVOLVEMENT:

- County Counsel for review
- Auditor for review and payments

FINANCING:

Financing for this lease payment will be the responsibility of Eastern Sierra Transit Authority, JPA but will credit Bishop Airport 150100 rents and leases 4311.

APPROVALS

COUNTY COUNSEL: AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS (Must be reviewed and approved by County Counsel prior to submission to the board clerk.)
Steve Sather Approved: yes Date 12/5/17

AUDITOR/CONTROLLER ACCOUNTING/FINANCE AND RELATED ITEMS (Must be reviewed and approved by the auditor/controller prior to submission to the board clerk.)
Chris Shepherd Approved: yes Date 12-8-17

PERSONNEL DIRECTOR PERSONNEL AND RELATED ITEMS (Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.)
Approved: _____ Date _____

DEPARTMENT HEAD SIGNATURE:
(Not to be signed until all approvals are received) William Date: 12/8/17

**COUNTY OF INYO - BISHOP AIRPORT
OFFICE AND COMMERCIAL SPACE LEASE**

THIS LEASE AGREEMENT, made and entered into this _____ day of _____, by and between **Eastern Sierra Transit Authority, JPA**, hereinafter referred to as "Lessee," and the County of Inyo, a political subdivision of the State of California, hereinafter referred to as "County," whereby the parties hereto agree as follows:

WITNESSETH:

SECTION ONE. ADMINISTRATION.

This Lease Agreement, hereinafter referred to as "Lease," shall be administered on behalf of the County by Shannon Williams, whose title is Deputy Public Works Director, hereinafter referred to as "County's Lease Administrator" and on behalf of Lessee by Lessee's Executive Director.

SECTION TWO. LEASED PREMISES.

County hereby leases to Lessee the real property (hereinafter referred to as "Leased Premises") located at the Bishop Airport (hereinafter referred to as "Airport"), County of Inyo, State of California, and described more particularly as: Approximately one thousand, one hundred and sixty-seven (1,167) square feet of office space and ten (1) "U's" of rack space in the terminal building as shown on Exhibit "A" attached hereto.

SECTION THREE. INITIAL TERM AND OPTIONS.

The initial term of the Lease will be for Two (2) years beginning December 1, 2017, and continuing through and including November 30, 2019. In addition to the initial term, there will be four (4) options to extend the Lease for additional one (1) year periods as follows:

- a. From December 1, 2019 through November 30, 2020.
- b. From December 1, 2020 through November 30, 2021.
- c. From December 1, 2021 through November 30, 2022.
- d. From December 1, 2022 through November 30, 2023.

The options to extend may be exercised in the manner and under the conditions hereinafter provided.

SECTION FOUR. EXERCISING OPTIONS TO EXTEND TERM.

The four (4) options to extend the term of the Lease for one (1) year periods identified in Section Three above, may be exercised by Lessee in the manner and on the terms and conditions below:

- a. Terms and Conditions.
- (1) Neither Lessee nor County has terminated this Lease, or any extensions thereof, for any reason.
 - (2) Lessee is not in default under any term or condition of the Lease, or any extension thereof.
 - (3) Lessee has exercised all previous options to extend.
- b. Manner In Which Option Can Be Exercised.
- (1) Lessee may exercise the option to extend no earlier than six (6) months before the expiration of the Lease term, or any extension thereof.
 - (2) Lessee must notify County in writing of the intent to exercise an option to extend at least thirty (30) days before the expiration of the Lease term, or an extension thereof.
 - (3) Except as provided for in Section Six relating to the rent, the Option to Extend shall be upon the same terms and conditions as stated in this Lease.

SECTION FIVE. HOLDING OVER.

If Lessee remains in possession of the Leased Premises with the consent of County, either expressed or implied, after the expiration of the Lease term, Lessee's tenancy shall be deemed to be a tenancy from month to month at the same rental rate applicable for the final month of the Lease term and otherwise shall be upon the same terms and conditions as are set forth in the Lease, provided that such tenancy shall be terminable and may be terminated upon at least thirty (30) days prior written notice of such termination served by either Lessee or County on the other party in the manner prescribed by law.

SECTION SIX. LEASE PAYMENTS.

Lessee will pay to County an annual Lease payment of Sixteen Thousand Five Hundred and Sixty Dollars (\$16,560.00). Lessee agrees to pay County said amount in monthly installments of One Thousand Three Hundred and Eighty Dollars (\$1380.00) per month, beginning on December 1, 2017, and payable on the first of each month thereafter during the term of this lease, or any extension thereof plus the following utilities: Electrical, propane, cleaning fees, trash pickup and supplies, and a \$50.00 payment for sign space, payment for which will be billed in arrears. If Lease payment is received more than ten (10) days after the date upon which it is due, a late payment equal to 5% of the lease payment shall be imposed.

In the event the Lessee exercises its option to extend the Lease for any or all of the four one-year periods, the rent for such option period may increase as agreed upon between County and Lessee, but such increase shall not exceed two and a half percent (2.5%) of the rent for the previous lease period. In the event County and Lessee do not agree upon a rental amount, the rent shall increase by the aforementioned percentage.

If the Lease or any extension thereof is terminated before the expiration of the complete term, the annual lease payment due will be prorated for the actual term of the Lease, or any extension thereof. If the Lessee holds over after the expiration of the Lease term, or any extension thereof, Lessee will pay County monthly rent at the rate of one-tenth (0.10) of the annual lease payment, for each month, or part thereof, in which Lessee holds over. Such monthly rent shall be

due on the first day of each month during which Lessee holds over.

SECTION SEVEN. USE OF PREMISES.

The premises are leased to be used for Administrative offices of the Eastern Sierra Transit Authority. Lessee agrees to restrict its use to such purposes, and not to use or permit the use of the premises for any other purpose without first obtaining the consent in writing of County.

SECTION 8. MASTER LEASE.

The property herein leased by County to Lessee is the subject of a master lease between County and the Department of Water and Power of the City of Los Angeles, Numbered BL 120, and by this reference incorporated into this Lease. This Lease by the County of Inyo is subject to all of the terms and conditions imposed upon County by said master lease, and Lessee hereunder hereby agrees to abide by all of the terms of said master lease.

SECTION NINE. DELIVERY OF POSSESSION.

Delivery of possession shall be deemed completed as of the date of execution of this instrument. Lessee represents and warrants that Lessee has examined the Leased Premises, including all buildings and improvements thereon and that as of the effective date of the lease, they are all in good order, repair, and in safe and clean condition.

SECTION TEN. QUIET POSSESSION.

The County covenants and agrees that Lessee, upon payment of the annual Lease payment and compliance with all the terms and conditions of this Lease, may lawfully, peacefully, and quietly have, hold, use, occupy, and enjoy the leased premises and each part thereof during the term of this Lease and any extensions thereof without hindrance or interruption by County.

SECTION ELEVEN. PARKING.

Lessee shall have reasonable non-exclusive use of the Airport parking area in common with other tenants, occupants, and users of the Airport, together with the right of reasonable ingress and egress to the Airport parking area.

SECTION TWELVE. HOURS OF USE.

Lessee shall have access to the leased premises at any time on a twenty-four hour per day, seven-day per week basis.

SECTION THIRTEEN. UTILITIES.

Lessee shall provide and pay for such electricity, lighting, heating, ventilation and all other utilities as are necessary for the reasonable use and enjoyment of the leased premises by the Lessee except as provided below. All charges for other utilities used by Lessee in connection with the occupancy of the leased premises, (including deposits, connection fees or charges, meter rentals as required by the supplier of any such utility service, and the cost of the facilities for connecting the leased premises to such utility service facilities) shall be paid by Lessee. County shall provide electrical service to those leased premises which cannot be separately metered for service.

SECTION FOURTEEN. JANITORIAL SERVICES.

Lessee shall furnish at its sole expense janitorial services which may be required on its

leased premises. Such services shall be provided at the level necessary to maintain the leased premises in a clean and orderly condition.

SECTION FIFTEEN. REPAIRS AND MAINTENANCE.

Lessee will maintain the leased premises and keep them in good repair at Lessee's own expense except that County shall maintain and repair the following portions of the leased premises: Exterior walls, roof, plumbing, heating, and ventilating. Lessee shall be responsible to maintain and repair all other portions of the leased premises not maintained by the County, including but not limited to the following: floors, interior walls, ceiling, windows, and doors, which will be maintained in a similar condition as exists at the effective date of this Lease, excepting reasonable wear and tear or damage that may be caused by "Acts of God". The County shall not be responsible for the maintenance and/or repair of any structure or improvement placed on the leased premises by the Lessee, in which case Lessee shall be solely responsible for the maintenance and/or repair of those structures and improvements.

When the County notifies Lessee that facilities within Lessee's area of responsibility are in need of repairs, Lessee will make such repairs within thirty (30) days of receiving the notification. If the nature of the repairs are such that they must be performed immediately in order to provide for the immediate safety of the public or airport users, Lessee will perform such emergency repairs immediately. If Lessee is unable to perform such emergency repairs immediately, the County reserves the right to make such repairs itself, or hire a contractor to make such repairs, at Lessee's expense.

SECTION SIXTEEN. ENTRY FOR INSPECTION AND MAINTENANCE.

County reserves the right to enter the leased premises at reasonable times, with twenty-four (24) hour prior notification to the Lessee, to inspect, to perform required maintenance and repair, or to make additions or alterations to any part of the premises. County also reserves the right to enter the leased premises at any time without prior notice to the Lessee in the event that an emergency reasonably requires the County to do so. Lessee agrees to permit County to do so. County may, during such time as is reasonably necessary to either respond to an emergency or to make such alterations, additions, or repairs, erect scaffolding, fences, and similar structures, post relevant notices, and place movable equipment without any obligation to reduce Lessee's rent for the demised premises during such period, and without incurring liability to Lessee for disturbance of quiet enjoyment of the premises, or loss of occupation thereof.

SECTION SEVENTEEN. ALTERATIONS AND IMPROVEMENTS.

Lessee shall make no alterations or improvements in or on the Leased Premises without the prior written consent of County. All alterations and improvements made by Lessee, other than removable personal property, shall remain on the Leased Premises and be deemed to be property of County upon the expiration or sooner termination of the Lease, unless otherwise agreed in writing by Lessee and County. Any damage occasioned by the installation or removal of Lessee's personal property shall be repaired by Lessee.

SECTION EIGHTEEN. SIGNS.

Lessee may erect signs necessary to identify Lessee's occupancy of the leased premises during the term hereunder. Lessee shall not place the proposed signs on the leased premises until County has reviewed the proposed design and given its consent to the proposed signs. County shall not unreasonably withhold said consent. Signs shall be removed by Lessee at the termination of this Lease.

SECTION NINETEEN. WASTE.

Lessee shall give prompt notice to County of any damages to the leased premises and shall not commit, or suffer to be committed, any waste or injury, or allow any public or private nuisance on the leased premises.

SECTION TWENTY. FIRE INSURANCE.

County will procure and maintain fire and extended coverage insurance on all buildings on the leased premises. Such insurance will be solely for the County's benefit. Lessee will have no right, title, or interest in such policy or in payments made to County under such policy.

SECTION TWENTY-ONE. DAMAGE OR DESTRUCTION.

In the event that the leased premises shall be totally or partially damaged by an event which is covered by the insurance policy described in Section Twenty during the term of this Lease or extension thereof, other than through the fault or neglect of Lessee, repairs shall be made by County at County's sole expense, with all reasonable dispatch. In the event that damage by such event, other than through the fault or negligence of Lessee, amounts to substantial destruction of the leased premises which cannot be repaired in three (3) months, this Lease may be terminated by either party at its option by giving written notice of intention to the other party within thirty (30) days following said destruction. If this Lease is not so terminated, Lessee shall be entitled to a pro rata reduction in the annual Lease payment to be jointly agreed upon by County and Lessee. If the leased premises are damaged or destroyed through the sole fault or negligence of Lessee or its employees, agents, invitees, or sublessees, this Lease may not be terminated by Lessee, and it shall be the obligation of Lessee, at its sole expense, to reconstruct or repair said leased premises.

SECTION TWENTY-TWO. COMMERCIAL INSURANCE REQUIREMENTS.

For the duration of this lease, Lessee shall procure and maintain insurance of the scope and amount specified in Attachment A and with the provisions specified in that attachment.

SECTION TWENTY-THREE. INDEMNIFICATION/HOLD HARMLESS.

23.1 Indemnity. Lessee will indemnify, hold harmless and defend County, its agents and employees, and its Lessor, the City of Los Angeles, its agents and employees, from and against any and all actions, claims, damages, disabilities or expenses including, without limitation, attorneys' fees, witness costs and court costs that may be asserted by any person or entity, including Lessee, arising out of or in connection with any of the following circumstances:

23.1.1 Use of Premises. Use of premises or Airport in any manner by Lessee, its agents, employees, invitees, subtenants, licensees and contractors, and the agents, employees, patrons, contractors and invitees of Lessees and subtenants, including any use of the premises or the Airport not allowed under this Lease.

23.1.2 Breach by Lessee. Any breach by Lessee of the terms, covenants or conditions herein contained.

23.1.3 Other Activities. Any other activities, including the direct or indirect release or spill of any legally designated hazardous material or waste on the leased premises, of Lessee, its agents, employees, invitees, and subtenants whether or not there is concurrent negligence on the part of the County, but excluding liability due to the sole active negligence or sole willful misconduct of the County. This indemnification obligation is not limited in any way by any limitation on the amount or type of damages or compensation payable by or for Lessee or its agents under workers' compensation acts, disability benefit acts or other employee benefit acts.

23.1.4. Exculpation of County. County, its officers, agents, and employees shall not be liable to Lessee for any loss or damage to Lessee or Lessee's property from any cause. Lessee expressly waives all claims against County, its officers, agents and employees, for injury or damage to person or property arising for any reason regardless of whether or not there is concurrent passive or active negligence of County, its officers, agents, and employees, unless such injury or damage is caused due to the sole active negligence or willful misconduct of County, its officers, agents, and employees.

SECTION TWENTY-FOUR. COMPLIANCE WITH LAW.

Lessee shall, at its sole cost, comply with all requirements of all County, State and Federal ordinances, laws, rules, and regulations now in force, or which may hereafter be in force, pertaining to the use of leased premises, and shall faithfully observe and obey all County, State and Federal ordinances, laws, rules, and regulations now in force, or which hereafter may be in force. If Lessee's failure to obey and comply with any of these rules, laws, ordinances, or regulations results in any assessment of fines, penalty, or damages against the County, Lessee will pay such civil penalty, fines or assessments and any costs the County incurs in defending or adjudicating such violations.

SECTION TWENTY-FIVE. TAXES, ASSESSMENTS, AND FEES.

In accordance with Revenue and Taxation Code section 107.6, Lessee is hereby advised that this lease may create a possessory interest subject to property taxation and that, if such an interest is created, Lessee is solely responsible for the payment of all property taxes levied on that interest. In addition, Lessee shall timely pay all taxes and assessments of whatever character that may be levied or charged upon the leasehold estate in the Leased Premises, or upon Lessee's operations thereon. Lessee shall also pay all license or permit fees that may be necessary, or which may be required by law, for the conduct of its operations at the Leased Premises.

SECTION TWENTY-SIX. GRANT AGREEMENT ASSURANCES.

The following assurances required by the Federal Government as a condition of the Grant Agreement for the Bishop Airport are hereby incorporated into, and made a condition of, this Lease:

a. The Lessee, for himself, his heirs, personal representatives, successors in interest, and assigns, as a part of the consideration hereof, does hereby covenant and agree as a covenant running with the land that in the event facilities are constructed, maintained, or otherwise operated on the said property described in this Lease for a purpose for which a DOT program or activity is extended or for another purpose involving the provision of similar services or benefits, the Lessee shall maintain and operate such facilities and services in compliance with all requirements imposed pursuant to Title 49, Code of Federal Regulations, DOT, Subtitle A, Office of the Secretary, Part 21, Nondiscrimination in Federally-Assisted Programs of the Department of Transportation-Effectuation of Title VI of the Civil Rights Act of 1964, and as said Regulations may be amended.

b. The Lessee, for himself, his personal representatives, successors in interest, and assigns, as a part of the consideration hereof, does hereby covenant and agree as a covenant running with the land that:

(1) No person on the grounds of race, color, or national origin shall be excluded from participation in, denied the benefits of, or be otherwise subjected to discrimination in the use of said facilities;

(2) That in the construction of any improvements on, over, or under such land and the furnishing of services thereon, no person on the grounds of race, color, or national origin shall be excluded from participation in, denied the benefits of, or otherwise be subject to discrimination;

(3) That the Lessee, licensee, permittee, etc. shall use the premises in compliance with all other requirements imposed by or pursuant to Title 49, Code of Federal Regulations, Department of Transportation, Subtitle A, Office of the Secretary, Part 21, Non-discrimination in Federally-Assisted Programs of the Department of Transportation-Effectuation of Title VI of the Civil Rights Acts of 1964, and as said Regulations may be amended.

c. In the event of a breach of any of the above nondiscrimination covenants, County shall have the right to terminate the Lease, and to re-enter and repossess said land and the facilities thereon, and hold the same as if said Lease had never been made or issued. This provision does not become effective until the procedures of 49 CFR Part 21 are followed and completed, including expiration of appeal rights.

d. Lessee shall furnish its accommodations and/or services on a fair, equal, and not unjustly discriminatory basis to all users thereof, and it shall charge fair, reasonable, and not unjustly discriminatory prices for each unit or services; provided that Lessee may be allowed to make reasonable and nondiscriminatory discounts, rebates, or other similar type of price reductions to volume purchasers.

e. Non-compliance with provisions of paragraph "d." above shall constitute a material breach hereof, and in the event of such non-compliance, the County shall have the right to terminate this Lease and the estate hereby created without liability therefore, or at the election of the County or the United States either or both said Governments shall have the right to judicially enforce those provisions.

f. Lessee agrees that it shall insert the above five provisions (paragraphs "a.", "b.", "c.", "d.", and "e.") in any lease, agreement, contract, or similar instrument, by which said Lessee grants a right or privilege to any person, firm, or corporation to render accommodations and/or services to the public on the premises herein leased.

g. Lessee assures that it will undertake an affirmative action program as required by 14 CFR Part 152, Subpart E, to insure that no person shall on the grounds of race, creed, color, national origin, or sex be excluded from participating in any employment activities covered in 14 CFR Part 152, Subpart E. Lessee assures that no person shall be excluded on these grounds from participating in or receiving the services or benefits of any program or activity covered by this subpart. Lessee assures that no person shall be excluded on these grounds from participating in or receiving the services or benefits of any program or activity covered by this subpart. Lessee assures that it will require that its covered sub-organizations provide assurances to Lessee that they similarly will undertake affirmative action programs and that they will require assurances from their sub-organizations, as required by 14 CFR 152, Subpart E, to the same effect.

h. County reserves the right to further develop or improve the landing area of the airport as it sees fit, regardless of the desires or view of Lessee, and without interference or hindrance.

i. County reserves the right to maintain and keep in repair all publicly owned facilities of the airport, together with the right to direct and control all activities of Lessee in this regard.

j. This Lease shall be subordinate to the provisions and requirements of any existing or future agreement between County and the United States relative to the development, operation, or maintenance of the airport.

k. There is hereby reserved to County, its successors and assigns, for the use and benefit of the public, a right of flight for the passage of aircraft in the airspace above the surface of the premises herein Leased. This public right of flight shall include the right to cause in said airspace any landing at, taking off from, or operation on the Airport.

l. Lessee agrees to comply with the notification and review requirements covered in Part 77 of the Federal Aviation Regulations in the event future construction of a building is planned for the Leased premises, or in the event of any planned modification or alteration of any present or future building or structure situated on the Leased premises.

m. Lessee, by accepting this Lease, expressly agrees for itself, its successors and assigns, that it will not erect or permit the erection of any structure or object, or permit the growth of any tree on the land leased hereunder, above the height set forth in Part 77 of Federal Aviation Regulations. In the event the aforesaid covenants are breached, County reserves the right to enter upon the land leased hereunder and to remove the offending structure or object or cut the offending tree, all of which shall be at the expense of Lessee.

n. Lessee, by accepting this Lease, agrees for itself, its successors and assigns, that it will not make use of the leased premises in any manner which might interfere with the landing and taking off of aircraft from the Airport, or otherwise constitute a hazard. In the event the aforesaid covenant is breached, County reserves the right to enter upon the premises hereby leased and cause the abatement of such interference at the expense of Lessee.

o. It is understood and agreed that nothing herein contained shall be construed to grant or authorize the granting of an exclusive right within the meaning of Section 308a of the Federal Aviation Act of 1958 (49 U.S.C. 1349a).

SECTION TWENTY-SEVEN. MODIFICATION.

The terms and conditions of the Lease and any extension thereof may be modified, changed, or amended at any time only by the mutual written consent of Lessee and County. However, County may, upon 30 days notice to Lessee, amend this Lease as a result of any modification or change in the Master Lease referenced in Section Eight herein, so long as such amendment is limited to an incorporation of the changes and/or modification to the Master Lease. The amended Lease shall take effect 30 days after Lessee is served with the amended Lease.

SECTION TWENTY-EIGHT. TERMINATION.

This Lease may be canceled and terminated by either party, without penalty, for any reason, at any time after execution of this Lease. Such cancellation and termination shall be effective on the sixtieth (60th) day after one party gives to the other written notice of termination. However, the giving of such notice shall not release either the County or the Lessee from full and faithful performance of all covenants of this Lease during the period between the giving of notice and the effective date of cancellation and termination.

SECTION TWENTY-NINE. RETURN OF PROPERTY AT TERMINATION.

Lessee will return the property in good condition upon termination or expiration of the Lease.

SECTION THIRTY. ASSIGNMENT AND SUBLEASE.

Lessee agrees not to assign this Lease or sublet the leased premises in part, or encumber its leasehold estate, or any interest therein, or permit the same to be occupied by another, either voluntarily or by operation of law, without first obtaining the written consent of County, which consent shall not be unreasonably withheld. Any such assignment or sublease shall not release Lessee from liability hereunder, and any assignee or sublessee shall expressly assume all Lessee's obligations hereunder. It is also agreed that the giving of a written consent required herein on any one or more occasions shall not thereafter operate as a waiver of the requirement for written consent on any one or more subsequent occasions.

SECTION THIRTY-ONE. SUBORDINATION.

Lessee agrees that this Lease shall be subject and subordinate to any mortgage, trust deed, or like encumbrance heretofore or hereafter placed upon the leased premises by County, or its successors in interest, to secure the payment of monies loaned, interest thereon, and other obligations. Lessee agrees to execute and deliver, upon demand of County, any and all instruments desired by County subordinating in the manner requested by County this Lease to such mortgage, trust deed, or like encumbrance.

Notwithstanding such subordination, Lessee's right to quiet possession of the leased premises shall not be disturbed if Lessee is not in default and so long as Lessee shall pay the rent and observe and perform all of the provisions in this Lease, unless this Lease is otherwise terminated pursuant to its terms.

SECTION THIRTY-TWO. MECHANIC'S LIEN.

Lessee agrees to keep the leased premises free from all mechanics' liens or other liens of like nature arising because of work done or materials furnished upon the leased premises at the instance of, or on behalf of Lessee, provided however that Lessee can contest such lien provided it post an adequate bond therefore.

SECTION THIRTY-THREE. FORCE MAJEURE.

If either party hereto shall be delayed or prevented from their performance of any act required hereunder by acts of God, restrictive governmental laws or regulations, strikes, civil disorders, or other causes not involving the fault, and beyond the control, of the party obligated (financial inability excepted), performance of such act shall be waived for the period of the delay. However, nothing in this clause shall excuse the Lessee from the payment of any rental or other charge required of Lessee, except as may be expressly provided elsewhere in this Lease.

SECTION THIRTY-FOUR. WAIVER.

It is agreed that any waiver by Lessee of any breach of any one or more of the covenants, conditions, or terms of this Lease shall not be construed to be a waiver of any subsequent breach of the same or different provision of the Lease; nor shall any failure on the part of the Lessee to require exact, full, complete, and explicit compliance with any of the covenants or conditions of this Lease be construed as in any manner changing the terms hereof, nor shall the terms of this Lease

be changed or altered in any way whatsoever other than by written amendment, signed by both parties.

SECTION THIRTY-FIVE. DEFAULT.

In the event that Lessee or County shall default in any term or condition of this Lease, and shall fail to cure such default within thirty (30) days following service upon the defaulting party of a written notice of such default specifying the default or defaults complained of, or if the default cannot reasonably be cured within thirty (30) days, the defaulting party fails to commence curing the default within thirty (30) days and thereafter to diligently and in good faith continue to cure the default, the complaining party may forthwith terminate this Lease by serving the defaulting party written notice of such termination.

SECTION THIRTY-SIX. INUREMENT.

The Lease shall be binding upon and inure to the benefit of the parties hereto and their respective heirs, executors, administrators, legal representatives, successors, and assigns.

SECTION THIRTY-SEVEN. SEVERABILITY.

If any provision of this Lease or the application thereof to any person or circumstances shall, to any extent, be invalid or unenforceable, the remainder of this Lease, or the application of such provisions to person or circumstances other than those as to which it is invalid or unenforceable, shall not be affected thereby, and each provision of this Lease shall be valid and be enforced to the fullest extent permitted by law.

SECTION THIRTY-EIGHT. TIME IS OF ESSENCE.

Time is expressly declared to be of the essence in this Lease and in all of the covenants and conditions herein.

SECTION THIRTY-NINE. ADDITIONAL TERMS AND CONDITIONS.

Additional terms and conditions of the Lease, if any, are set forth in the exhibits listed below, each of which is attached hereto and incorporated herein by this reference: Exhibit A, Exhibit B, Exhibit C, and Exhibit D

SECTION FORTY. AMENDMENT.

The Lease may be amended only by a written document signed by all parties hereto.

SECTION FORTY-ONE. ENTIRE AGREEMENT.

The Lease contains the entire agreement between the parties hereto and supersedes all previous agreements between the parties with respect to the subject matter of the Lease.

SECTION FORTY-TWO. CONSTRUCTION OF AGREEMENT.

Both County and Lessee have had the opportunity to and have participated in the drafting and final preparation of this Lease agreement. For that reason, the Lease itself, or any ambiguity contain therein, shall not be construed against either the County or Lessee as the drafters of this document.

SECTION FORTY-THREE. NOTICE.

Any notice required by the Lease or applicable law to be given or served on Lessee or County may be given or served either by personal delivery to the County Lease Administrator or any one of the Lessees, by personal delivery to, or by depositing the notice in the United States Mail, postage prepaid, to the address of each party as given below:

COUNTY

Public Works Deputy Director
168 N. Edwards St., P.O. Drawer Q
Independence, CA 93526

**Department
Address
City and State**

LESSEE

Eastern Sierra Transit Authority
703 B Airport Road, P.O. Box 1357
Bishop, CA 93514

**Name
Address
City and State**

**COUNTY OF INYO - BISHOP AIRPORT
OFFICE AND COMMERCIAL SPACE LEASE**

Initial Term of Lease:
December 1, 2017 through November 30, 2019

IN WITNESS THEREOF, the parties hereto have set their hands and seals this _____
day of _____, 20_____.

COUNTY

LESSEE

Lease Administrator

By _____
Director, Department of Public Works

Signature

Type or Print Name

Date: _____

Date: _____

Approved as to form and legality:

County Counsel

Approved as to accounting form and content:

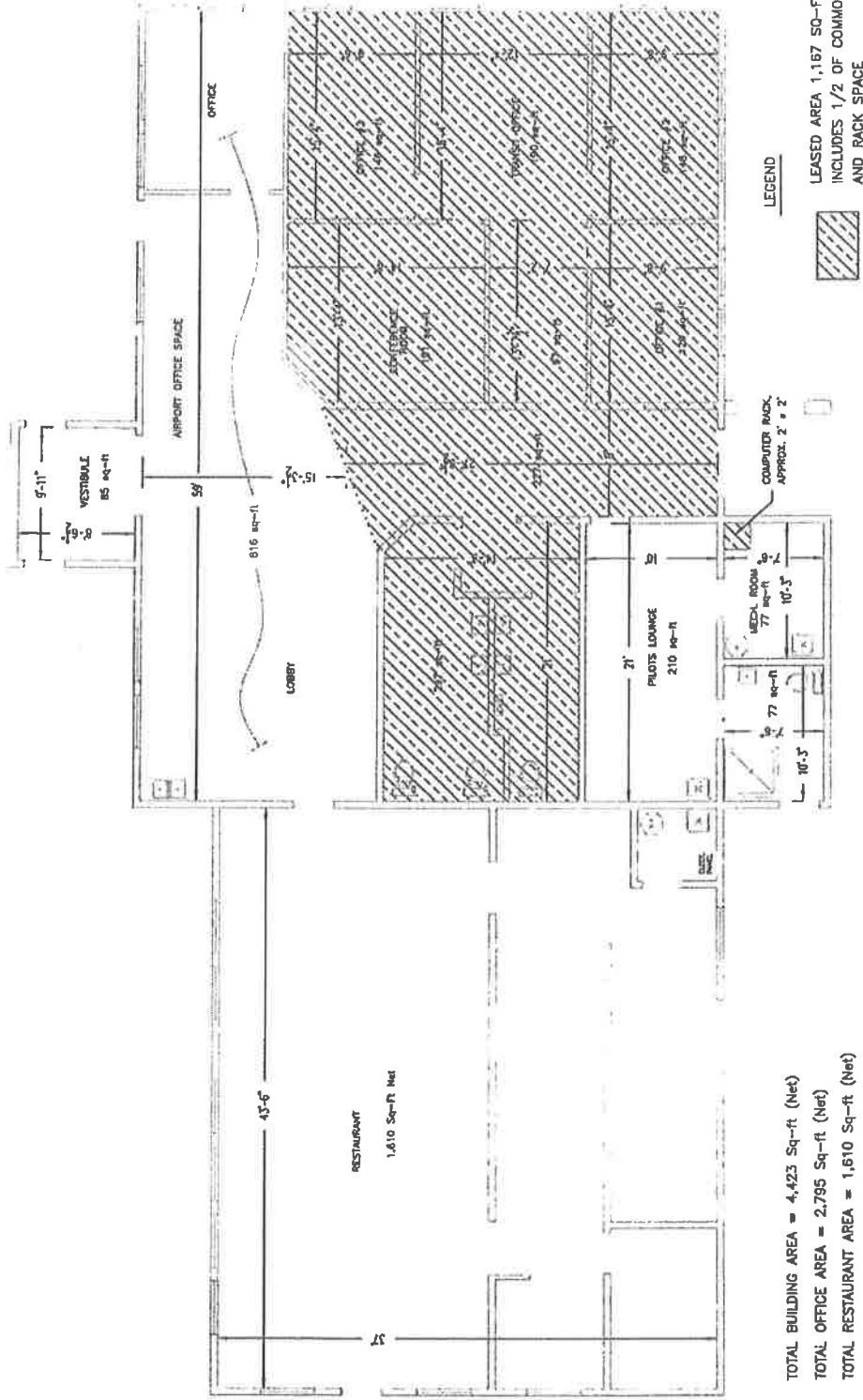
County Auditor

Approved as to insurance and risk management:

County Risk Manager

s:CountyCounsel/Leases

EXHIBIT A



Prepared by: DAYO COUNTY PUBLIC WORKS 188 N. Edwards, P.O. Drawer 0 Independence, CA 93526 (760) 878-0201		BISHOP AIRPORT TERMINAL BUILDING ESTA LEASE		DATE: JAN. 2011		DRAWING NO. 10-10-10-001		FLOOR PLAN	
Checked by: J. Anderson 2-11-10	Drawn by: A. Anderson 10-15-10	Design by: A. Anderson 2-11-10	Date: 2-11-10	Scale: 1/8" = 1'	Title: FLOOR PLAN	Author: A. Anderson	Date: 2-11-10	Project: Bishop Airport Terminal Building Esta Lease	Drawing No.: 10-10-10-001

Exhibit B
Airport Office and Commercial Lease
Eastern Sierra Transit Authority

1. Description of the Eastern Sierra Transit Authority (ESTA) Office Lease Space

ESTA Office Space (Net Space – does not include walls)	
Conference Room	191 sq. ft.
Office #1	129 sq. ft.
Office #2	148 sq. ft.
Office #3	146 sq. ft.
Transit Office	190 sq. ft.
Hallway #2	97 sq. ft.
Computer Rack Space in Mechanic Room	4 sq. ft.
Total	905 sq. ft.

2. Common Space at Bishop Airport Terminal

ESTA Common Space at Bishop Airport Terminal	
Hallway	227 sq. ft.
Restrooms	297 sq. ft.
Total	524 sq. ft.

The lease rate for common space is 50% of the regular least rate. Therefore, ESTA will only be billed for 50% of 524 square feet or 262 square feet.

3. Total Office Lease Area

Office Space	905 sq. ft.
Common Space	262 sq. ft.
Total Square Feet	1,167 sq. ft.

ATTACHMENT A

COUNTY OF INYO

Bishop

AIRPORT

OFFICE AND COMMERCIAL SPACE LEASE

SEE ATTACHED INSURANCE PROVISIONS

COMMERCIAL INSURANCE REQUIREMENTS

Lessee shall procure and maintain for the duration of the contract insurance against claims for injuries to persons or damages to property which may arise from or in connection with the Lessee's operation and use of the leased premises. The cost of such insurance shall be borne by the Lessee.

A. Minimum Scope and Limit of Insurance

Coverage shall be at least as broad as:

1. **Commercial General Liability (CGL):** Insurance Services Office Form CG 00 01 covering CGL on an "occurrence" basis, including property damage, bodily injury and personal injury with limits no less than **\$2,000,000** per occurrence. If a general aggregate limit applies, either the general aggregate limit shall apply separately to this project/location or the general aggregate limit shall be twice the required occurrence limit.
2. **Workers' Compensation** insurance as required by the State of California, with Statutory Limits, and Employer's Liability Insurance with limits of no less than **\$1,000,000** per accident for bodily injury or disease. (for lessees with employees).
3. **Auto Liability:** ISO Form Number CA 00 01 covering any auto (Code 1) or if Lessee has no owned autos, hired (Code 8), and non-owned autos (code 9), with limits no less than \$500,000 per accident for bodily injury and property damage.
4. **Property insurance** against all risks of loss to any tenant improvements or betterments, at full replacement cost with no coinsurance penalty provision.

If the Lessee maintains higher limits than the minimums shown above, the Entity requires and shall be entitled to coverage for the higher limits maintained.

B. Other Insurance Provisions:

The policies are to contain, or be endorsed to contain, the following provisions:

1. For General Liability, the Entity, its officers, officials, employees, and volunteers are to be **covered as additional insureds** with respect to liability arising out of ownership, maintenance, or use of that part of the premises leased to the lessee.
2. The Lessee's insurance coverage shall be **primary insurance** as respects the Entity, its officers, officials, employees and volunteers. Any insurance or self-insurance maintained by the Entity, its officers, officials, employees, or volunteers shall be excess of the Lessee's insurance and shall not contribute with it.
3. Each insurance policy required above shall contain, or be endorsed to contain, a waiver of all **rights of subrogation** against the Entity.
4. Each insurance policy shall be endorsed to state that coverage shall not be canceled except after thirty (30) days' prior written notice (10 days for non-payment) has been given to the Entity.
5. The Property insurance shall **name the Entity as Loss Payee** as its interests may appear.

C. Acceptability of Insurers

Insurance is to be placed with insurers with a current A.M. Best's rating of no less than A: VII, unless otherwise acceptable to the Entity.

D. Deductibles and Self-Insured Retentions

Any deductibles or self-insured retentions must be declared to and approved by the Entity. At the option of the Entity, either: the Lessee shall obtain coverage to reduce or eliminate such deductibles or self-insured retentions as respects the Entity, its officers, officials, employees, and volunteers; or the Lessee shall provide a financial guarantee satisfactory to the Entity guaranteeing payment of losses and related investigations, claim administration, and defense expenses.

E. Verification of Coverage

Lessee shall furnish the Entity with original certificates and amendatory endorsements or copies of the applicable policy language providing the insurance coverage required above. All certificates and endorsements are to be received and approved by the Entity before work commences. However, failure to obtain the required documents prior to the work beginning shall not waive the Lessee's obligation to provide them. The Entity reserves the right to require complete, certified copies of all required insurance policies, including endorsements, required by these specifications, at any time.

F. Waiver of Subrogation

Lessee hereby grants to Entity a waiver of any right to subrogation which any insurer of said Lessee may acquire against the Entity by virtue of the payment of any loss under such insurance. This provision applies regardless of whether or not the Entity has received a waiver of subrogation endorsement from the insurer.

G. Special Risks or Circumstances

Entity reserves the right to modify these requirements at any time, including limits, based on the nature of the risk, prior experience, insurer, coverage, or other special circumstances.



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

For Clerk's Use Only: AGENDA NUMBER 22

- Consent Departmental Correspondence Action Public Hearing
 Scheduled Time for Closed Session Informational

FROM: County Administrator / County Counsel / Public Works

FOR THE BOARD MEETING OF: December 19, 2017

SUBJECT: Credit Rating Agreement

DEPARTMENTAL RECOMMENDATION:

Request your Board consider approving a Credit Rating Agreement with Inyo County Development LLC whereby it will obtain an updated credit rating for the County, the cost of which the County would potentially reimburse in the amount of \$20,000 under terms specified in the Agreement, and authorize the County Administrator to sign.

SUMMARY DISCUSSION:

Inyo County Development LLC ("ICD"), the developer of the proposed Consolidated County Office Building Project, is in the process of updating its cost estimates for the Project for consideration by the Board of Supervisors. This involves both updating construction costs and evaluating financing options. In seeking financing, the Developer has determined that the County having a current credit rating might influence the interest rate it can obtain in the private equity market by as much as a 100 basis points. The Developer is willing to fund the cost of obtaining a credit rating for the County, estimated at \$20,000, but has requested the County agree to reimburse its cost for obtaining the rating if ICD is ultimately able to offer the County a Basic Annual Rent (as part of the proposed lease agreement for the Project) that does not exceed five percent (5%) more than the Basic Annual Rent amount ICD most recently proposed but the County ultimately decides, for whatever reason, not to proceed with the project.

The County has not committed to proceeding with the Project, and is under no obligation to do so. In order to commit to proceeding with the Project, the Board of Supervisors will need to consider the lease for the Project in open session and, to do this, the County requires updated Project pricing information which will dictate the rent in the lease.

The Financial Advisory Committee has discussed and endorsed the merits of the County having an updated credit rating regardless of the Consolidated Office Building Project. The fact the County could obtain a new credit rating – the last formal credit rating was obtained in the Nineties as part of the County's refinancing of the Certificates of Participation for the Jail – possibly at no cost through this Credit Rating Agreement mechanism was also appealing to the members of the FAC. As such, the FAC voted 5-0 on Wednesday, December 6, 2017, to recommend to the Board of Supervisors that the County proceed with obtaining and updated credit rating for the County.

ALTERNATIVES:

Your Board could choose not to enter into the Credit Rating Agreement and not obtain a current credit rating for the County or pay for the credit rating upfront. The latter is not recommended because the Credit Rating

Agreement provides the County with a means of obtaining a credit rating at, possibly, no cost. The former is not recommended because (a), without the new credit rating, the revised costs for the proposed Consolidated Office Building Project are likely to be higher than they otherwise would be; and, (b) the County would lose the additional benefits of having a current credit rating for other financing issues related to the provision of public services.

OTHER AGENCY INVOLVEMENT:

Financial Advisory Committee; Inyo County Development LLC

FINANCING:

There is no cost associated with entering into the Credit Rating Agreement, however, if ICD is ultimately able to offer the County a Basic Annual Rent (as part of the proposed lease agreement for the consolidated office building) that does not exceed five percent (5%) more than the Basic Annual Rent amount ICD most recently proposed but the County nevertheless declines to enter into the proposed lease agreement, then the County will have an obligation to reimburse ICD \$20,000.

<u>APPROVALS</u>	
COUNTY COUNSEL:	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS <i>(Must be reviewed and approved by county counsel prior to submission to the board clerk.)</i> <div style="text-align: right; margin-top: 10px;"> Approved: <u>yes</u> Date <u>12/14/17</u> </div>
AUDITOR/CONTROLLER:	ACCOUNTING/FINANCE AND RELATED ITEMS <i>(Must be reviewed and approved by the auditor-controller prior to submission to the board clerk.)</i> <div style="text-align: right; margin-top: 10px;"> Approved: _____ Date _____ </div>
PERSONNEL DIRECTOR:	PERSONNEL AND RELATED ITEMS <i>(Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.)</i> <div style="text-align: right; margin-top: 10px;"> Approved: _____ Date _____ </div>

DEPARTMENT HEAD SIGNATURE:  Date: 12-14-2017
 (Not to be signed until all approvals are received)
 (The Original plus 20 copies of this document are required)

DEPARTMENT HEAD SIGNATURE:  Date: 12/14/17
 (Not to be signed until all approvals are received)
 (The Original plus 20 copies of this document are required)

Credit Rating Agreement

This Agreement is entered into this ___ day of December, 2017, by and between the County of Inyo, a political subdivision of the State of California ("the County") and Inyo County Development LLC, a Texas limited liability company ("ICD"). The County and ICD are sometimes referred to collectively herein as "the parties."

Recitals:

A. ICD and the County are in negotiations regarding revised price and terms of payment for a potential build-to-suit lease agreement pertaining to a consolidated office building in Bishop, California (the "Project").

B. ICD has represented to the County that it can provide a substantially better price and terms of payment if the County has a current credit rating from a qualified rating agency such as Standard and Poor's or Moody's.

C. ICD is willing to incur the costs necessary to obtain such a rating if the County agrees to reimburse those costs in an amount stipulated to be \$20,000, in the event that ICD is ultimately able to offer the County a Basic Annual Rent (as part of the proposed lease agreement) that does not exceed five percent (5%) more than the Basic Annual Rent amount ICD most recently proposed (as discussed below) but the County nevertheless declines to enter into the proposed lease agreement. It is understood that the County is under no obligation to enter into any lease agreement for the Project.

Terms and Conditions:

NOW, THEREFORE, the parties agree as follows:

1. Credit Rating Issuance. ICD will commit all resources to provide the appropriate scope of services for the purposes of obtaining a new credit rating for the County from either Moody's or Standard and Poor's. The County will cooperate in that effort and provide such documentation or other information as is ordinarily required by a ratings agency in connection with issuing a new credit rating. The parties anticipate that the process for obtaining such a rating will take ninety (90) days from the date first written above. The parties do not know what the rating will be and no provision of this Agreement is conditioned on a particular rating being issued.
2. Reimbursement Obligation ("False Start Provision"). After the rating is obtained, ICD will provide the County with a new proposed Basic Annual Rent for the proposed lease agreement, with all other substantive terms and conditions of the proposed lease

agreement not pertaining to Basic Annual Rent remaining consistent with the most recent draft exchanged by the parties (version 14). If that new proposed amount for Basic Annual Rent does not exceed five percent (5%) more than the Basic Annual Rent amount ICD most recently proposed but the County nevertheless chooses not to enter into the proposed lease agreement, then the County will reimburse ICD's costs of obtaining the credit rating in an amount stipulated by the parties to be twenty thousand dollars (\$20,000). For reference, the last Basic Annual Rent amount proposed by ICD for the lease agreement was Eight Hundred Forty-Nine Thousand Six Hundred and Forty-Eight Dollars (\$849,648.00) (which is a higher amount than that stated on the parties' original term sheet dated 11/6/13).

3. Entire Agreement. This Agreement contains the sole and entire agreement and understanding between the parties with respect to the entire subject matter hereof, and any and all prior discussions, negotiations, commitments, or understandings related hereto, whether oral or written, are hereby merged herein. Among other things, the parties agree that with the exception of the potential reimbursement obligation created by this Agreement, the County is under no obligation to reimburse ICD's or anyone else's costs incurred in connection with the proposed lease agreement or the Project in the event that the County chooses in its sole discretion not to enter into a lease agreement with them for the Project.

4. Counterparts. This Agreement may be executed in counterparts and, when executed, all such counterparts shall constitute one agreement that shall be binding upon the parties, notwithstanding that the signatures of the parties' designated representatives do not appear on the same page.

5. Notices. Any notices required by this Agreement shall be sent via e-mail to the addresses for the other party at the email addresses provided in this paragraph, or at such other address for a party as shall have been specified by the party in written notice provided to other party. Notices shall be addressed and delivered as follows:

To County:

County Administrator
P.O. Drawer N
Independence, California 93526
E-mail: kcarunchio@inyocounty.us

Copy to:
County Counsel
County of Inyo
P.O. Drawer M
Independence, California 93526
E-mail: mrudolph@inyocounty.us

To ICD:

Inyo County Development LLC
16250 Knoll Trail Drive, #102
Dallas, Texas 75248
E-mail: waynecharleslamb@gmail.com

6. Amendments and Waiver. No amendment or waiver of any provision of this Agreement, nor consent to any departure, shall be effective unless in writing and signed by each party, and then such waiver or consent shall be effective only in the specific instances and for the specific purpose given.
7. Choice of Law. This Agreement shall be interpreted and enforced pursuant to the laws of the State of California without regard to choice of law principles.
8. Interpretation. This Agreement is the product of negotiation and preparation by and among the parties and their respective counsel. It shall not be deemed prepared or drafted by one party or another, and shall be construed accordingly.
9. Illegality/Severability. Any provision or provisions of this Agreement that are determined by a court of competent jurisdiction to be invalid, void, or illegal, shall in no way affect, impair or invalidate any other provisions hereof, and the remaining provisions hereof shall nevertheless remain in full force and effect.
10. Headings. Section headings in this Agreement are included for convenience of reference only and shall not be given any substantive effect.
11. No Attorneys' Fees. The parties agree that, in any action to enforce the terms of this Agreement, each party shall bear its own attorneys' fees and costs.

Execution

IN WITNESS WHEREOF, the parties will be deemed to have executed this Agreement as of the date first written above.

COUNTY

By:

ICD

By: Wayne Lamb, Partner



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

For Clerk's Use Only: AGENDA NUMBER 23

- Consent Departmental Correspondence Action Public Hearing
 Scheduled Time for Closed Session Informational

FROM: Recycling and Waste Management

FOR THE BOARD MEETING OF: December 19, 2017

SUBJECT: Approval of Amendment No.1 to the agreement with Preferred Septic and Disposal, Inc. for waste hauling services at Olancha, Keeler and Darwin Transfer Stations.

DEPARTMENTAL RECOMMENDATION:

Request that your Board:

- 1.) Approve and Ratify Amendment No. 1 to the contract between the County of Inyo and Preferred Septic and Disposal, Inc. to start on July 1, 2017 increasing the contract limit payable under the agreement from \$116,496.00 to \$157,407.00, and modifying the schedule of fees for the Olancha, Keeler, and Darwin Waste Removal Contract; and
- 2.) Authorize the Chairperson to sign Amendment No. 1 for the Olancha, Keeler and Darwin Waste Removal Contract.

SUMMARY DISCUSSION:

On August 16, 2016 your Board entered into an agreement with Preferred Septic and Disposal, Inc. to provide for waste hauling services for Olancha, Keeler and Darwin transfer stations. The contract reflected the floor rate for hauling services in effect at the time. Now that the floor rates have increased it is necessary to adjust the agreements to reflect the change.

The attached amendment increases the not to exceed amount to conform to the new floor rate, resulting in an annual increase to the hauling rate for Olancha, Keeler and Darwin from \$38,433.00 per year to \$59,129.00 per year. The not to exceed amount includes two, \$980 per event, on-call illegal dumping cleanups per year for the remaining two years of this contract. This amendment does not alter any other terms or conditions of the contract.

ALTERNATIVES:



If the attached amendment is not approved by your Board the funding in the agreements will be inadequate to compensate the hauler for the full floor rate for waste hauling services which would require other arrangements to provide dumpsters and waste hauling at the Olancha, Keeler and Darwin transfer stations.

OTHER AGENCY INVOLVEMENT: None

FINANCING:

Funds for this service have been included in the Recycling and Waste Management Program recommended budget unit 045700.

APPROVALS

COUNTY COUNSEL: 	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS (Must be reviewed and approved by county counsel prior to submission to the board clerk.) Approved: <u>yes</u> Date <u>12/15/17</u>
AUDITOR/CONTROLLER: 	ACCOUNTING/FINANCE AND RELATED ITEMS (Must be reviewed and approved by the auditor-controller prior to submission to the board clerk.) Approved: <u>yes</u> Date <u>12/17/17</u>
PERSONNEL DIRECTOR:	PERSONNEL AND RELATED ITEMS (Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.) N/A Approved: _____ Date _____

REQUESTED BY: _____ Date: _____

DEPARTMENT HEAD SIGNATURE:  _____ Date: 12/14/17
(Not to be signed until all approvals are received)

**AMENDMENT NUMBER 1 TO
AGREEMENT BETWEEN THE COUNTY OF INYO AND
PREFERRED SEPTIC AND DISPOSAL, INC.
FOR THE PROVISION OF INDEPENDENT CONTRACTOR SERVICES**

WHEREAS, the County of Inyo (hereinafter referred to as "County") and PREFERRED SEPTIC AND DISPOSAL, INC., of BISHOP, CA (hereinafter referred to as "Contractor"), have entered into an Agreement for the Provision of Independent Contractor Services dated AUGUST 16, 2016, on County of Inyo Standard Contract No. 116, for the term from AUGUST 2, 2016 to JUNE 30, 2019.

WHEREAS, County and Contractor do desire and consent to amend such Agreement as set forth below;

WHEREAS, such Agreement provides that it may be modified, amended, changed, added to, or subtracted from, by the mutual consent of the parties thereto, if such amendment or change is in written form, and executed with the same formalities as such Agreement, and attached to the original Agreement to maintain continuity.

County and Contractor hereby amend such Agreement as follows:

D. LIMIT UPON AMOUNT PAYABLE UNDER AGREEMENT. The total sum of all payments made by the County to Contractor performed under this Agreement shall not exceed \$157,407 Dollars (hereinafter referred to as "contract limit") County expressly reserves the right to deny any payment or reimbursement requested by Contractor for services or work performed which is in excess of the contract limit.

ATTACHMENT B: SCHEDULE OF FEES

OLANCHA: 9 EACH, 4 CUBIC YARD DUMPSTERS FOR TRASH EMPTIED 2 TIMES PER WEEK:
PRICE PER CONTAINER = \$311.11 PER MONTH, TOTAL FOR 9 DUMPSTERS = \$2,799.99 PER MONTH

OLANCHA RECYCLING AS STATED IN SCOPE OF WORK: FREE OF CHARGE

KEELER: 8 EACH, 4 CUBIC YARD DUMPSTERS FOR TRASH EMPTIED 1 TIME PER WEEK:
PRICE PER CONTAINER = \$177.28 PER MONTH, TOTAL FOR 8 DUMPSTERS = \$1,418.24 PER MONTH

KEELER RECYCLING AS STATED IN SCOPE OF WORK: FREE OF CHARGE

DARWIN: 4 EACH, 4 CUBIC YARD DUMPSTERS FOR TRASH EMPTIED 1 TIME PER WEEK:
PRICE PER CONTAINER = \$177.28 PER MONTH, TOTAL FOR 4 DUMPSTERS = \$709.12 PER MONTH

DARWIN RECYCLING AS STATED IN SCOPE OF WORK: FREE OF CHARGE

ILLEGAL DUMPING AND BULKY ITEM CLEANUP: CHARGED AT \$980 PER CLEAN UP, ON-CALL SERVICE

5% SAVINGS FOR INVOICES PAID WITHIN 30 DAYS OF RECEIPT FOR TRASH SERVICES, EXCLUDES ILLEGAL DUMPING AND BULKY ITEM CLEANUP CHARGES.

The effective date of this Amendment to the Agreement is JULY 1, 2017.

All the other terms and conditions of the Agreement are unchanged and remain the same.

AMENDMENT NUMBER 1 TO
AGREEMENT BETWEEN THE COUNTY OF INYO AND
PREFERRED SEPTIC AND DISPOSAL, INC.
FOR THE PROVISION OF INDEPENDENT CONTRACTOR SERVICES

IN WITNESS THEREOF, THE PARTIES HERETO HAVE SET THEIR HANDS AND SEALS THIS
____ DAY OF _____, _____

COUNTY OF INYO

By: _____

Dated: _____

CONTRACTOR

By: Kristen Deam
Signature

Kristen Deam
Type or Print

Dated: 12-6-2017

APPROVED AS TO FORM AND LEGALITY:

Neuralb
County Counsel

APPROVED AS TO ACCOUNTING FORM:

County Auditor

APPROVED AS TO PERSONNEL REQUIREMENTS:

Personnel Services

APPROVED AS TO RISK ASSESSMENT:

UM Baker
County Risk Manager

**AMENDMENT NUMBER 1 TO
AGREEMENT BETWEEN THE COUNTY OF INYO AND
PREFERRED SEPTIC AND DISPOSAL, INC.
FOR THE PROVISION OF INDEPENDENT CONTRACTOR SERVICES**

IN WITNESS THEREOF, THE PARTIES HERETO HAVE SET THEIR HANDS AND SEALS THIS
DAY OF _____, _____.

COUNTY OF INYO

By: _____

Dated: _____

CONTRACTOR

By: _____

Signature

Type or Print

Dated: _____

APPROVED AS TO FORM AND LEGALITY:

County Counsel

APPROVED AS TO ACCOUNTING FORM:



County Auditor

APPROVED AS TO PERSONNEL REQUIREMENTS:

Personnel Services

APPROVED AS TO RISK ASSESSMENT:



County Risk Manager



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

For Clerk's Use Only:
AGENDA NUMBER

24

- Consent
 Departmental
 Correspondence Action
 Public Hearing
 Scheduled Time for
 Closed Session
 Informational

FROM: Kevin D. Carunchio, County Administrator

FOR THE BOARD MEETING: December 19, 2017

SUBJECT: Continuation of declaration of existence of local emergency

DEPARTMENTAL RECOMMENDATION:

Request Board discuss and consider staff's recommendation regarding continuation of the local emergency known as the "Here It Comes Emergency" that was proclaimed in anticipation of run-off conditions from near-record snowpack posing extreme peril to the safety of property and persons in Inyo County.

SUMMARY DISCUSSION:

During your March 28, 2017 Board of Supervisors meeting your Board took action to approve Resolution 2017-15 proclaiming the existence of a local emergency, which has been named the Here It Comes Emergency, in anticipation of run-off conditions from near-record snowpack posing extreme peril to the safety of property and persons in Inyo County and which are likely beyond the control of the services, personnel, equipment and facilities of the County of Inyo. During your June 27, 2017 meeting, your Board took action to amend Resolution 2017-15 to recognize that the County has moved from the Preparedness stage to the Response stage, and to include new damages and impacts that have occurred in the operational area.

In light of the massive amount of runoff that is occurring due to the unprecedented snowpack, the recommendation is that the emergency be continued on a biweekly basis and that Resolution 2017-15 be updated as necessary, until further evaluation of conditions are completed and staff makes the recommendation to end the emergency.

ALTERNATIVES: N/A

OTHER AGENCY INVOLVEMENT: N/A

FINANCING: N/A

APPROVALS

COUNTY COUNSEL: N/A	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS <i>(Must be reviewed and approved by county counsel prior to submission to the board clerk.)</i> Approved: _____ Date _____
AUDITOR/CONTROLLER: N/A	ACCOUNTING/FINANCE AND RELATED ITEMS <i>(Must be reviewed and approved by the auditor-controller prior to submission to the board clerk.)</i> Approved: _____ Date _____
PERSONNEL DIRECTOR: N/A	PERSONNEL AND RELATED ITEMS <i>(Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.)</i> Approved: _____ Date _____

DEPARTMENT HEAD SIGNATURE:

(Not to be signed until all approvals are received)

(The Original plus 20 copies of this document are required)

Date: 12-08-17



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

For Clerk's Use Only:
AGENDA NUMBER
 25

- Consent
 Departmental
 Correspondence Action
 Public Hearing
 Scheduled Time for
 Closed Session
 Informational

FROM: Kevin D. Carunchio, County Administrator

FOR THE BOARD MEETING: December 19, 2017

SUBJECT: Continuation of declaration of local emergency

DEPARTMENTAL RECOMMENDATION:

Request Board discuss and consider staff's recommendation regarding continuation of the local emergency known as the "Rocky Road Emergency" that was proclaimed as the result of flooding, mud, and rock landslides and deep snow drifts over portions of Inyo County caused by an atmospheric river weather phenomena that began January 3, 2017 and continued throughout February.

SUMMARY DISCUSSION:

During your February 7, 2017 Board of Supervisors meeting your Board took action to approve Resolution 2017-04 declaring a local emergency, which has been named The Rocky Road Emergency, and was the result of an atmospheric river weather phenomena that began January 3, 2017 and caused flooding, mud, and rock landslides and deep snow drifts over portions of Inyo County. Since the circumstances and conditions relating to this emergency persist, your Board directed that the continuation of the declaration be considered on a biweekly basis. On March 7, 2017, your Board amended Resolution 2017-04 to further extend the continuation of the emergency and also add language to include additional damages that occurred in the latter half of January and into February.

ALTERNATIVES: N/A

OTHER AGENCY INVOLVEMENT: N/A

FINANCING: N/A

APPROVALS

COUNTY COUNSEL: N/A	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS <i>(Must be reviewed and approved by county counsel prior to submission to the board clerk.)</i> Approved: _____ Date _____
AUDITOR/CONTROLLER: N/A	ACCOUNTING/FINANCE AND RELATED ITEMS <i>(Must be reviewed and approved by the auditor-controller prior to submission to the board clerk.)</i> Approved: _____ Date _____
PERSONNEL DIRECTOR: N/A	PERSONNEL AND RELATED ITEMS <i>(Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.)</i> Approved: _____ Date _____

DEPARTMENT HEAD SIGNATURE:

(Not to be signed until all approvals are received)

(The Original plus 20 copies of this document are required)

Date: 12-08-17



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

For Clerk's Use Only:
AGENDA NUMBER
 26

- Consent Departmental Correspondence Action Public Hearing
 Scheduled Time for Closed Session Informational

FROM: Kevin D. Carunchio, County Administrator
By: Kelley Williams, Assistant to the CAO

FOR THE BOARD MEETING OF: December 19, 2017

SUBJECT: Discussion on Discontinuation or Modification of Land of EVEN Less Water Local Emergency Proclamation

DEPARTMENTAL RECOMMENDATION:

Request Board discuss and consider staff's recommendation to continue the local emergency known as the "Land of EVEN Less Water Emergency," that was proclaimed as a result of extreme drought conditions that existed until recently in the County, while considering how to address the ongoing hydrologic issues in West Bishop.

SUMMARY DISCUSSION:

On January 17, 2014, Governor Brown proclaimed a State of Emergency and directed state officials to take all necessary actions to prepare for the forthcoming water shortfalls and drought conditions, due to the driest year in recorded state history. During your January 28, 2014 meeting your Board took action to concurrently approve Resolution 2014-09 proclaiming a local emergency, named the "Land of EVEN Less Water Emergency," a result of the severe and extreme drought conditions that existed in Inyo County. On June 28, 2016, your Board amended Resolution 2014-09 to include language to address the high groundwater saturation problems that were occurring in the West Bishop area due to the fluctuation in hydrologic conditions.

On April 7, 2017, due to the unprecedented water conservation and plentiful winter rain and snow, Governor Brown ended the drought state of emergency in most of California, while maintaining water reporting requirements and prohibitions on wasteful practices. Executive Order B-40-17 lifts the drought emergency except in areas where emergency drinking water projects will continue to help address diminished groundwater supplies. Executive Order B-40-17 also builds on actions taken in Executive Order B-37-16, which remains in effect, to continue to make water conservation a way of life in California.

As discussed at your Board meeting of April 18, 2017, due to the changed circumstances and conditions relating to this state and local emergency, it is recommended that the local emergency known as "The Land of Even Less Water" be modified – rather than discontinued outright – so that considerations can still be in place to address the ongoing hydrologic issues in West Bishop. At that meeting, your Board voted to continue the emergency for the time being, until staff can present a modified version to take into account the West Bishop situation. Staff is recommending the Board take the same action today.

ALTERNATIVES: N/A

OTHER AGENCY INVOLVEMENT: N/A

FINANCING: N/A

APPROVALS

COUNTY COUNSEL: N/A	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS <i>(Must be reviewed and approved by county counsel prior to submission to the board clerk.)</i> Approved: _____ Date _____
AUDITOR/CONTROLLER: N/A	ACCOUNTING/FINANCE AND RELATED ITEMS <i>(Must be reviewed and approved by the auditor-controller prior to submission to the board clerk.)</i> Approved: _____ Date _____
PERSONNEL DIRECTOR: N/A	PERSONNEL AND RELATED ITEMS <i>(Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.)</i> Approved: _____ Date _____

DEPARTMENT HEAD SIGNATURE:
 (Not to be signed until all approvals are received)

[Handwritten Signature]

Date: 12-08-17



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

For Clerk's Use Only:
AGENDA NUMBER
 27

- Consent
 Departmental
 Correspondence Action
 Public Hearing
 Scheduled Time for
 Closed Session
 Informational

FROM: Kevin D. Carunchio, County Administrator

FOR THE BOARD MEETING: December 19, 2017

SUBJECT: Continuation of declaration of local emergency

DEPARTMENTAL RECOMMENDATION:

Request Board discuss and consider staff's recommendation regarding continuation of the local emergency, known as the "Gully Washer Emergency," that resulted in flooding in the central, south and southeastern portion of Inyo County during the month of July, 2013.

SUMMARY DISCUSSION:

During your August 6, 2013 Board of Supervisors meeting your Board took action to declare a local emergency, which has been named The Gully Washer Emergency, which was a result of flooding in the central, southern and southeastern portion of Inyo County during the month of July. Since the circumstances and conditions relating to this emergency persist, your Board directed that the continuation of the declaration be considered on a biweekly basis. The recommendation is that the emergency be continued until the further evaluation of the damage is completed and staff makes the recommendation to end the emergency.

ALTERNATIVES: N/A

OTHER AGENCY INVOLVEMENT: N/A

FINANCING: N/A

APPROVALS

COUNTY COUNSEL: N/A	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS <i>(Must be reviewed and approved by county counsel prior to submission to the board clerk.)</i> Approved: _____ Date _____
AUDITOR/CONTROLLER: N/A	ACCOUNTING/FINANCE AND RELATED ITEMS <i>(Must be reviewed and approved by the auditor-controller prior to submission to the board clerk.)</i> Approved: _____ Date _____
PERSONNEL DIRECTOR: N/A	PERSONNEL AND RELATED ITEMS <i>(Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.)</i> Approved: _____ Date _____

DEPARTMENT HEAD SIGNATURE:

(Not to be signed until all approvals are received)

(The Original plus 20 copies of this document are required)

Date: 12-08-17



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

For Clerk's Use Only:
AGENDA NUMBER
 28

- Consent
 Departmental
 Correspondence Action
 Public Hearing
 Scheduled Time for
 Closed Session
 Informational

FROM: Kevin D. Carunchio, County Administrator

FOR THE BOARD MEETING OF: December 19, 2017

SUBJECT: Continuation of proclamation of local emergency

DEPARTMENTAL RECOMMENDATION:

Request Board discuss and consider staff's recommendation regarding continuation of the local emergency, known as the "Death Valley Down But Not Out Emergency," that was proclaimed as a result flooding in the central, south and southeastern portion of Inyo County during the month of October, 2015.

SUMMARY DISCUSSION:

During your October 27, 2015 Board of Supervisors meeting your Board took action to proclaim a local emergency, which has been named the Death Valley Down But Not Out Emergency that is a result of flooding in the central, south and southeastern portion of Inyo County. Since the circumstances and conditions relating to this emergency persist, the recommendation is that the emergency be continued on a biweekly basis, until the further evaluation of the damage is completed and staff makes the recommendation to end the emergency.

ALTERNATIVES: N/A

OTHER AGENCY INVOLVEMENT: N/A

FINANCING: N/A

APPROVALS

COUNTY COUNSEL: N/A	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS <i>(Must be reviewed and approved by county counsel prior to submission to the board clerk.)</i> Approved: _____ Date _____
AUDITOR/CONTROLLER: N/A	ACCOUNTING/FINANCE AND RELATED ITEMS <i>(Must be reviewed and approved by the auditor-controller prior to submission to the board clerk.)</i> Approved: _____ Date _____
PERSONNEL DIRECTOR: N/A	PERSONNEL AND RELATED ITEMS <i>(Must be reviewed and approved by the director of personnel services prior to submission to the board clerk.)</i> Approved: _____ Date _____

DEPARTMENT HEAD SIGNATURE:

(Not to be signed until all approvals are received)

(The Original plus 20 copies of this document are required)



Date: 12-08-17



AGENDA REQUEST FORM
BOARD OF SUPERVISORS
COUNTY OF INYO

For Clerk's Use Only:
AGENDA NUMBER
29

- Consent Hearing
 Departmental
 Correspondence Action
 Public
 Scheduled Time for
 Closed Session
 Informational

FROM: HEALTH & HUMAN SERVICES – Public Health and Prevention

FOR THE BOARD MEETING OF:

SUBJECT: Tobacco Control Presentation and Request for Direction

DEPARTMENTAL RECOMMENDATION:

Request Board receive a presentation regarding new funding and associated requirements for the tobacco control program and provide direction to staff for development of Tobacco Control Agreement and associated tobacco control plan.

CAO RECOMMENDATION:

SUMMARY DISCUSSION:

Proposition 56, the Tobacco Tax Initiative of 2016, was passed by California voters on November 8, 2016, increasing the CA tobacco tax from \$0.84 to \$2.84 per pack. A portion of this significant increase in tobacco tax revenue is allocated to Local Lead Agencies (in most cases this is the Local Health Department) to support mandated Tobacco Control efforts pursuant to Health and Safety Code 104400.

Tobacco use remains the number one cause of preventable death, disease, and disability in the U.S., and tobacco use affects not only direct users of tobacco, but also non-smokers exposed to secondhand and thirdhand smoke as well as the environment. Tobacco-related diseases cause approximately 16% of deaths in California each year. In addition, California taxpayers spend \$3.58 billion dollars each year to treat cancer and other smoking-related diseases.

The goal of the California Tobacco Control Program (CTCP) is to change the social norms surrounding tobacco use in order to make tobacco less desirable, less acceptable, and less accessible. CTCP focuses on policy, system, and environmental change rather than individual behavior change as a way to use funds most effectively and efficiently for the greatest impact on society.

California has the longest running comprehensive tobacco control program in the nation. Since the program began with the passage of Prop 99 in 1988, smoking prevalence has steadily declined, with adult smoking prevalence declining from 23.7% in 1988 to 11.6% in 2014. As a result of statewide and local initiatives, California has the second lowest adult smoking prevalence rate in the U.S., second only to Utah. However, high-risk groups in California, such as rural populations, continue to suffer disproportionately from tobacco-related illnesses and death.

Due to new research and analysis of declining smoking rates, public health advocates are beginning to envision and promote "endgame" strategies to completely eliminate the tobacco epidemic, with a goal of ending tobacco use by 2035. Strategies include tobacco excise tax increases, secondhand smoke protections, mass media campaigns, interventions targeted towards vulnerable populations, tobacco use cessation benefits, and raising the legal age of tobacco sales to 21.

In Inyo County, the allocation for Tobacco control has increased from \$150,000.00 in FY 16/17 to \$369,105.00 in FY 17/18. Annual funding will decrease in subsequent years due to the anticipated decrease in tobacco tax revenue as more and more Californian's quit smoking.

FY 17/18 marks the first year of a 4-year plan for Tobacco Control in each county. Additional Tobacco Control program requirements have been established by the California Department of Public Health (CDPH):

- Required objectives are similar to prior 4-year funding cycle, including two policy objectives (one must focus on

- retail environment), and maintaining established adult and youth tobacco coalitions.
- With new funding, the activities under each objective increase.
- New opportunity to add objectives, including cessation.
- Increased requirements for FTE and external program evaluation.

Inyo County is required to submit a new plan and budget to CDPH and sign an allocation agreement to receive funds and acknowledge the program requirements.

HHS is asking your Board for direction on the following options:

1. Continue to provide tobacco control and either
 - a. Implement the required objectives using county staff and possible contracts with other agencies, or
 - b. Pass all funding to non-county non-profit agencies in order to have all of the required objectives implemented by contracted agencies, or
2. Reject the tobacco allocation via non-compliance with the LLA funding agreement, which will mean that CDPH will be required to identify another county or non-profit agency to contract with to implement the mandated Tobacco Control program in Inyo County.

HHS recommends that your Board allow county staff and contractors to implement the requirements of the program, as identified in Option #1, above. This will allow HHS to bring the Tobacco Allocation Agreement before your Board, complete negotiations with CDPH, finalize the local tobacco control plan and budget for FY 17/18, make any necessary mid-year budget revisions, move forward with plans to make changes to departmental authorized strength (conditioned upon additional approval from your Board) and initiate contracts for specific objectives and external evaluation.

ALTERNATIVES:

Your Board could choose other options not recommended by HHS, including contracting all tobacco control activities to non-profit agencies, reject tobacco control funding via non-compliance (e.g. non-acceptance of tobacco allocation agreement), or direct staff to pursue options not presented today.

OTHER AGENCY INVOLVEMENT:

Juvenile Probation, Behavioral Health, Inyo County Superintendent of Schools, Bishop Union High School, Home Street Middle School, Lone Pine High School, Lo-Inyo Elementary, Big Pine High School, Owens Valley School, Round Valley School, Toiyabe Indian Health Project, Owens Valley Career Development Center, Bishop Indian Education Center.

FINANCING:

State and Federal funding for the local Tobacco Control Education Program is \$369,105.00 for FY 17/18. If the allocation is accepted, funds will be brought into the Tobacco Prevention budget (640315) in State Grants (4498) as reported on the reimbursement requests submitted to the State. No County General Fund.

<u>APPROVALS</u>	
COUNTY COUNSEL:	AGREEMENTS, CONTRACTS AND ORDINANCES AND CLOSED SESSION AND RELATED ITEMS <i>(Must be reviewed and approved by County Counsel prior to submission to the Board Clerk.)</i> Approved: _____ Date: _____
AUDITOR/CONTROLLER:	ACCOUNTING/FINANCE AND RELATED ITEMS <i>(Must be reviewed and approved by the Auditor/Controller prior to submission to the Board Clerk.)</i> Approved: _____ Date: _____
PERSONNEL DIRECTOR:	PERSONNEL AND RELATED ITEMS <i>(Must be reviewed and approved by the Director of Personnel Services prior to submission to the Board Clerk.)</i> Approved: _____ Date: _____
BUDGET OFFICER:	BUDGET AND RELATED ITEMS <i>(Must be reviewed and approved by the Budget Officer prior to submission to the Board Clerk.)</i> Approved: _____ Date: _____

DEPARTMENT HEAD SIGNATURE: *Maulyn Mamm by Jody Uellen* Date: 12/8/17
 (Not to be signed until all approvals are received)

Inyo County HHS Tobacco Control Program FY 2017-18



**PRESENTED BY HHS-PUBLIC HEALTH AND
PREVENTION DIVISION**

Tobacco Control in CA



- **Brief history of accomplishments**
 - Longest running tobacco control program in the nation
 - Focus on social norms rather than individual behavior change
 - Second lowest adult smoking in the nation, second to Utah
- **Why is this important to Public Health**
 - #1 cause of preventable death and disease
 - Affects direct users, non-smokers, and the environment
 - Costs to taxpayers

Prop 56 Tobacco Tax- Additional Funding, New Requirements



- Original Tobacco Allocation from Prop 99 [1996]:\$150,000
- With new Prop 56 Funding [2017]:

FY 16/17	FY 17/18	FY 18/19	FY 19/20	FY 20/21
\$150,000	\$369,105	\$318,270	\$311,550	\$305,085

- Keep existing required objectives, expand activities under each
 - Retail Objective
 - Policy Objective
 - Coalitions (adult/youth)
- Opportunity to add objectives (e.g. Cessation)
- New guidelines re. min. FTE, external evaluation, min. expenditures for media.

Additional Funding, New Requirements, cont.



- 100% FTE Project Director/Project Coordinator
- 50%-100% FTE Coalition and Community Engagement Coordinator
- Min 10% FTE Internal Evaluation (may be Project Director)
- Min 10% FTE External Evaluator
- Independent Fiscal and Compliance Audit
- Min 10% of annual allocation must be spent on evaluation
- Min 3 Objectives (may expanded activities under existing required objectives and may add objectives)
 - Required: 2 Policy/Systems change objectives
 - Required: Healthy Stores for Health Community objective
 - Required: objectives must address priority populations and coalition development/Maintenance/Community Engagement
 - Optional: up to 10% may be used for direct cessation services

Context and Options



Per HSC Section 104400, Local Health Department is the designated Local Lead Agency (LLA)

LLAs are required to accept Tobacco Control Program funds and implement a comprehensive tobacco control program

Option 1: Accept Tobacco Allocation

- a. Implement with County staff, with option to contract out some objectives/activities [**Recommended**]
- b. County pass through- all objectives implemented by contractor

Option 2: Reject Funding via non-compliance (all or nothing re. Prop 99 + Prop 56 funds)

- Local tobacco control program mandate remains whether the program is administered by the County of Inyo or a different government or non-profit agency

Option	Advantage	Disadvantage	Impact
<p>1a- Accept funding, County staff and contractor mix</p> <p>*Recommended*</p>	<p>Continue to make progress toward tobacco control goals</p> <p>Benefit from staff experience</p> <p>Maintain Established programing and partnerships</p>	<p>Stringent requirements (min FTE, % req. for eval, legislated policy objectives)</p> <p>Additional staffing needed to meet objectives</p>	<p>Increase staffing</p> <p>Increase Tobacco Control activities</p> <p>Expand Youth Coalition</p> <p>Add Cessation Services</p>
<p>1b- Accept funding, contract out</p>	<p>Spread money to other organizations</p> <p>Limit county staffing</p>	<p>Burden of administrative and fiscal oversight remains</p> <p>County still ultimately responsible for meeting program requirements</p>	<p>Staff reduction (TBD)</p> <p>May limit control of quality/quantity of prevention services</p>
<p>2- Reject funds at local level via noncompliance</p>	<p>State takes on mandate of ensuring tobacco control program continues in Inyo</p>	<p>No change in required local objectives</p> <p>Less input from County re how and what tobacco control activities are prioritized</p>	<p>Staff reduction (0.8 FTE)</p> <p>Less control over quality/quantity of prevention services, policy advocacy</p>

Option 1a- Recommended



- Add 1 FTE (Contract Employee-Human Services Supervisor) in order to meet Project Director minimum FTE requirement and to oversee implementation of plan/internal evaluation
 - Maintain 0.5 FTE (or higher) county employee to help address objectives, especially in support of adult and youth coalitions and community engagement
 - Initiate external evaluation contract Request for Proposals
 - Partner with other County Departments, such as Probation, to purchase staff time to address some objectives (e.g. tobacco cessation)
- AND/OR**
- Contract out specific objectives and/or activities to community non-profit agencies that target priority populations

Option 1b



- Spread funding to local non-profit and other partner agencies
- Retain staff time to administer funding distribution, monitor performance, reporting
- HHS would still be ultimately responsible for ensuring all of the required objectives, activities, evaluation, and reporting are completed
- Contract funding level will be dependent on performance toward required objectives, and therefore cannot be guaranteed

Option 2



- **Reject Tobacco Control Funding (via non-compliance)**
 - No mechanism for rejecting the funding
 - LLA funding agreement may be terminated by CDPH if Local Health Department is non-compliant with enabling legislation or CDPH guidelines for tobacco control programs
 - ✦ This has happened in Merced County, but the county is lobbying to regain LLA designation
 - If LLA funding agreement is terminated, CDPH will reallocate funds to a different governmental agency or private non-profit within the jurisdiction
 - ✦ Same requirements as for LLA including policy, retail, coalition objectives
 - County loses any say in who gets the funding