

# STATE OF ALASKA INVITATION TO BID (ITB)



## OFFICE OF CHILDREN'S SERVICES CONFIDENTIAL PRINTING AND MAILING SERVICES

ITB 2025-2600-0251

ISSUED 01/08/2025

THE OFFICE OF CHILDREN'S SERVICES (OCS) SEEKS A QUALIFIED VENDOR FOR THE PRINTING AND MAILING OF ITS  
CONFIDENTIAL NOTIFICATIONS.

**IMPORTANT NOTICE:** If you received this solicitation from the State of Alaska's "Online Public Notice" web site, you must register with the procurement officer listed below if you desire to receive notification of subsequent amendments to the solicitation.

**BIDDER'S NOTICE:** By signature on this form, the bidder certifies that they comply with the following:

- (1) the bidder has a valid Alaska business license or will obtain one prior to award of any contract resulting from this ITB. If the bidder possesses a valid Alaska business license, the license number must be written below or one the following forms of evidence must be submitted with the bid:
  - a canceled check for the business license fee;
  - a copy of the business license application with a receipt date stamp from the State's business license office;
  - a receipt from the State's business license office for the license fee;
  - a copy of the bidder's valid business license;
  - a sworn notarized affidavit that the bidder has applied and paid for a business license;
- (2) the price(s) submitted was arrived at independently and without collusion, under penalty of perjury, and that the bidder is complying with:
  - the laws of the State of Alaska;
  - the applicable portion of the Federal Civil Rights Act of 1964;
  - the Equal Employment Opportunity Act and the regulations issued thereunder by the state and federal government;
  - the Americans with Disabilities Act of 1990 and the regulations issued thereunder by the state and federal government;
  - the bid will remain open and valid for at least 90 days;
  - all terms and conditions set out in this Invitation to Bid (ITB).

If a bidder does not hold an Alaska Business License (1) at the time designated in the ITB for opening the state will disallow the Alaska Bidder Preference. Bids must also be submitted under the name as appearing on the bidder's current Alaska business license in order to receive the Alaska Bidder Preference. If a bidder fails to comply with (2) of this paragraph, the state may reject the bid, terminate the contract, or consider the contractor in default.

<b>DEPARTMENT OF FAMILY AND COMMUNITY SERVICES</b>	
OFFICE OF CHILDREN'S SERVICES	COMPANY SUBMITTING BID
PROCUREMENT OFFICER:	AUTHORIZED SIGNATURE
<b>DANI OLSEN</b>	PRINTED NAME
PHONE: (907) <b>465-8216</b>	
EMAIL: dani.olsen@alaska.gov	DATE

# TABLE OF CONTENTS

<b>SECTION 1. INTRODUCTION &amp; INSTRUCTIONS .....</b>	<b>4</b>
SEC. 1.01 PURPOSE OF THE ITB.....	4
SEC. 1.02 BUDGET .....	4
SEC. 1.03 DEADLINE FOR RECEIPT OF BIDS .....	4
SEC. 1.04 PRIOR EXPERIENCE .....	4
SEC. 1.05 REQUIRED REVIEW.....	4
SEC. 1.06 QUESTIONS PRIOR TO DEADLINE FOR RECEIPT OF BIDS .....	4
SEC. 1.07 SITE INSPECTION.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
SEC. 1.08 RETURN INSTRUCTIONS.....	5
SEC. 1.09 ASSISTANCE TO BIDDERS WITH A DISABILITY.....	5
SEC. 1.10 AMENDMENTS TO BIDS .....	5
SEC. 1.11 AMENDMENTS TO THE ITB .....	5
SEC. 1.12 ITB SCHEDULE .....	5
SEC. 1.13 PRE-BID CONFERENCE/TELECONFERENCE .....	6
SEC. 1.14 ALTERNATE BIDS .....	6
SEC. 1.15 SUPPORTING INFORMATION.....	6
SEC. 1.16 FIRM, UNQUALIFIED, AND UNCONDITIONAL OFFER .....	6
<b>SECTION 2. SCOPE OF WORK AND CONTRACT INFORMATION .....</b>	<b>7</b>
SEC. 2.01 SCOPE OF WORK.....	7
SEC. 2.02 CONTRACT TERM .....	8
SEC. 2.03 CONTRACT TYPE .....	8
SEC. 2.04 PAYMENT FOR STATE PURCHASES .....	9
SEC. 2.05 ELECTRONIC PAYMENTS .....	9
SEC. 2.06 PROMPT PAYMENT FOR STATE PURCHASES.....	9
SEC. 2.07 CONTRACT ADMINISTRATION .....	9
SEC. 2.08 CONTRACT PRICE ADJUSTMENTS .....	9
SEC. 2.09 CONTRACT PERFORMANCE LOCATION .....	10
SEC. 2.10 THIRD-PARTY FINANCING AGREEMENTS NOT ALLOWED.....	10
SEC. 2.11 SUBCONTRACTORS.....	10
SEC. 2.12 JOINT VENTURES.....	11
SEC. 2.13 RIGHT TO INSPECT PLACE OF BUSINESS .....	11
SEC. 2.14 F.O.B. POINT .....	11
SEC. 2.15 INSPECTION & MODIFICATION - REIMBURSEMENT FOR UNACCEPTABLE DELIVERABLES .....	11
SEC. 2.16 EQUIPMENT INSPECTION .....	11
SEC. 2.17 NEW EQUIPMENT .....	11
SEC. 2.18 REMANUFACTURED/RECONDITIONED EQUIPMENT.....	12
SEC. 2.19 LEMON CLAUSE .....	12
SEC. 2.20 DISCONTINUED ITEMS .....	12
SEC. 2.21 LIQUIDATED DAMAGES .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
SEC. 2.22 SHIPPING DAMAGE.....	12
SEC. 2.23 CONTRACT CHANGES – UNANTICIPATED AMENDMENTS .....	12
SEC. 2.24 CONTINUING OBLIGATION OF CONTRACTOR .....	12
SEC. 2.25 BILLING INSTRUCTIONS .....	13
SEC. 2.26 ESTIMATED QUANTITIES .....	13
SEC. 2.27 WARRANTY .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
SEC. 2.28 NONDISCLOSURE AND CONFIDENTIALITY .....	13
SEC. 2.29 INDEMNIFICATION .....	14
SEC. 2.30 INSURANCE .....	14
<b>SECTION 3. BID FORMAT AND CONTENT .....</b>	<b>16</b>
SEC. 3.01 BID FORMS .....	16
SEC. 3.02 BID BOND – PERFORMANCE BOND – SURETY DEPOSIT .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
SEC. 3.03 PRICES.....	16
<b>SECTION 4. EVALUATION AND CONTRACTOR SELECTION.....</b>	<b>17</b>
SEC. 4.01 EVALUATION OF BIDS.....	17
SEC. 4.02 APPLICATION OF PREFERENCES .....	17
SEC. 4.03 ALASKA BIDDER PREFERENCE .....	17
SEC. 4.04 ALASKA VETERAN PREFERENCE.....	18
SEC. 4.05 ALASKA MILITARY SKILLS PROGRAM PREFERENCE.....	18
SEC. 4.06 USE OF LOCAL FOREST PRODUCTS.....	19
SEC. 4.07 LOCAL AGRICULTURAL AND FISHERIES PRODUCT PREFERENCE.....	19
SEC. 4.08 ALASKA PRODUCT PREFERENCE .....	19

SEC. 4.09	EMPLOYMENT PROGRAM PREFERENCE .....	20
SEC. 4.10	ALASKANS WITH DISABILITIES PREFERENCE .....	20
SEC. 4.11	PREFERENCE QUALIFICATION LETTER .....	21
SEC. 4.12	EXTENSION OF PRICES .....	21
SEC. 4.13	METHOD OF AWARD .....	21
SEC. 4.14	CONTRACTOR SELECTION PROCESS .....	21
SEC. 4.15	NOTICE OF INTENT TO AWARD .....	21
<b>SECTION 5.</b>	<b>GENERAL PROCESS AND LEGAL INFORMATION.....</b>	<b>22</b>
SEC. 5.01	INFORMAL DEBRIEFING .....	22
SEC. 5.02	ALASKA BUSINESS LICENSE AND OTHER REQUIRED LICENSES .....	22
SEC. 5.03	AUTHORITY .....	22
SEC. 5.04	COMPLIANCE .....	23
SEC. 5.05	SUITABLE MATERIALS, ETC. ....	23
SEC. 5.06	SPECIFICATIONS .....	23
SEC. 5.07	BRAND SPECIFIC .....	23
SEC. 5.08	ITEM UPGRADES .....	23
SEC. 5.09	WORKMANSHIP AND MATERIALS.....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
SEC. 5.10	CONTRACTOR SITE INSPECTION .....	23
SEC. 5.11	ORDER DOCUMENTS .....	23
SEC. 5.12	HUMAN TRAFFICKING .....	24
SEC. 5.13	RIGHT OF REJECTION .....	24
SEC. 5.14	STATE NOT RESPONSIBLE FOR PREPARATION COSTS.....	24
SEC. 5.15	DISCLOSURE OF BID CONTENTS .....	25
SEC. 5.16	ASSIGNMENTS.....	25
SEC. 5.17	FORCE MAJEURE (IMPOSSIBILITY TO PERFORM) .....	25
SEC. 5.18	DEFAULT .....	25
SEC. 5.19	DISPUTES .....	26
SEC. 5.20	SEVERABILITY .....	26
SEC. 5.21	CONTRACT CANCELLATION .....	26
SEC. 5.22	GOVERNING LAW; FORUM SELECTION .....	26
SEC. 5.23	QUALIFIED BIDDERS .....	26
SEC. 5.24	FEDERALLY IMPOSED TARIFFS .....	26
SEC. 5.25	PROTEST .....	27
<b>SECTION 6.</b>	<b>ATTACHMENTS .....</b>	<b>29</b>
SEC. 6.01	ATTACHMENTS .....	29

## **SECTION 1. INTRODUCTION & INSTRUCTIONS**

### **SEC. 1.01 PURPOSE OF THE ITB**

The Department of Family and Community Services, Office of Children’s Services, is soliciting bids to establish a term contract for the printing and mailing of its confidential notifications.

### **SEC. 1.02 BUDGET**

Department of Family and Community Services, Office of Children’s Services, estimates a budget \$355,000.00 dollars for the overall length of the contract. **Bids priced at more than \$355,000.00 will be considered non-responsive.**

Approval or continuation of a contract resulting from this ITB is contingent upon legislative appropriation.

### **SEC. 1.03 DEADLINE FOR RECEIPT OF BIDS**

Bids must be received no later than 5:00pm Alaska Time on 01/27/2025, at which time they will be publicly opened. Late bids or amendments will be considered non-responsive and will not be opened or accepted for evaluation.

### **SEC. 1.04 PRIOR EXPERIENCE**

In order for a bid to be considered responsive the bidder must meet these minimum prior experience requirements:

- Vendors must complete **Required Vendor Response - DFCS IT Requirements**, which correspond to the requirements described in Section 3 of this document, and return it as part of their proposal. A failure to complete and return this IT Reference will result in a proposal being deemed non-responsive.
- Vendor must meet the State and DFCS standards for Data Destruction Requirements.

A bidder's failure to meet these minimum prior experience requirements will cause their bid to be considered non-responsive and rejected.

### **SEC. 1.05 REQUIRED REVIEW**

Bidders shall carefully review this ITB for defects and questionable or objectionable material. Comments concerning defects and questionable or objectionable material in the ITB should be made in writing and received by the procurement officer at least ten days before the deadline for receipt of bids. This will allow time for an amendment to be issued if one is required. It will also help prevent the opening of a defective bid, upon which award cannot be made, and the resultant exposure of bidders' prices.

### **SEC. 1.06 QUESTIONS PRIOR TO DEADLINE FOR RECEIPT OF BIDS**

All questions must be in writing and directed to the procurement officer. The interested party must confirm telephone conversations in writing. Two types of questions generally arise. One may be answered by directing the questioner to a specific section of the ITB. These questions may be answered over the telephone. Other questions

may be more complex and may require a written amendment to the ITB. The procurement officer will make that decision.

### **SEC. 1.07 RETURN INSTRUCTIONS**

Bidders must submit via email, the entire bid may be emailed to [fcs.fms.vendor.response@alaska.gov](mailto:fcs.fms.vendor.response@alaska.gov) and must contain the ITB number in the subject line of the email. The **maximum** size of a single email (including all text and attachments) that can be received by the state is **20MB (megabytes)**. If the email containing the bid exceeds this size, the bid must be sent in multiple emails that are each less than 20 MB and each email must comply with the requirements described above.

Please note that email transmission is not instantaneous. Like sending a hard copy bid, if you are emailing your bid, the state recommends sending it enough ahead of time to ensure the email is delivered by the deadline for receipt of bids.

It is the bidder's responsibility to contact the issuing agency at (907) 465-8216 to confirm that the entire bid has been received. The state is not responsible for unreadable, corrupt, or missing attachments.

### **SEC. 1.08 ASSISTANCE TO BIDDERS WITH A DISABILITY**

The State of Alaska complies with Title II of the Americans with Disabilities Act of 1990. Individuals with disabilities who may need auxiliary aids, services, and/or special modifications to submit a bid should contact the Procurement Officer no later than ten days prior to the closing of the bid to make any necessary arrangements.

### **SEC. 1.09 AMENDMENTS TO BIDS**

Amendments to or withdrawals of bids will only be allowed if acceptable requests are received prior to the deadline that is set for receipt of bids, in accordance with 2 AAC 12.140. No amendments or withdrawals will be accepted after the deadline unless the delay is due to an error of the contracting agency, in accordance with 2 AAC 12.160.

### **SEC. 1.10 AMENDMENTS TO THE ITB**

If an amendment is issued before the deadline for receipt of bids, the amendment will be posted on the State of Alaska Online Public Notice (OPN) website. The link to the posting of the amendment will be provided to all who were notified of the ITB and to those who have registered with the procurement officer after receiving the ITB from the OPN.

### **SEC. 1.11 ITB SCHEDULE**

The ITB schedule below represents the State of Alaska's best estimate of the schedule that will be followed. If a component of this schedule, such as the deadline for receipt of bids, is delayed, the rest of the schedule may be shifted accordingly. All times are Alaska Standard Time (AST).

<b>ACTIVITY</b>	<b>TIME</b>	<b>DATE</b>
Issue Date / ITB Released	10:00am	01/08/2025
Deadline for Receipt of Bids / Bid Due Date	5:00pm	01/27/2025
Bid Evaluations Complete	10:00am	01/29/2025
Notice of Intent to Award	5:00pm	01/29/2025
Contract Issued	5:00pm	02/07/2025

This ITB does not, by itself, obligate the state. The state's obligation will commence when the contract is approved by the Commissioner of the Department of Family and Community Services, or the Commissioner's designee. Upon written notice to the contractor, the state may set a different starting date for the contract. The state will not be responsible for any work done by the contractor, even work done in good faith, if it occurs prior to the contract start date set by the state.

#### **SEC. 1.12 PRE-BID CONFERENCE/TELECONFERENCE**

A pre-bid conference will not be held for this ITB.

#### **SEC. 1.13 ALTERNATE BIDS**

Bidders may only submit one bid for evaluation. In accordance with 2 AAC 12.830 alternate bids (bids that offer something different than what is asked for) will be rejected.

#### **SEC. 1.14 SUPPORTING INFORMATION**

Provided a bid meets the requirements for a definite, firm, unqualified, and unconditional offer, the state reserves the right to request supplemental information from the bidder, after the bids have been opened, to ensure that the products or services offered completely meet the ITB requirements. The requirement for such supplemental information will be at the reasonable discretion of the state and may include the requirement that a bidder will provide a sample product(s) so that the state can make a first-hand examination and determination.

A bidder's failure to provide this supplemental information or the product sample(s), within the time set by the state, may cause the state to consider the offer non-responsive and reject the bid.

#### **SEC. 1.15 FIRM, UNQUALIFIED, AND UNCONDITIONAL OFFER**

To be responsive a bid must constitute a definite, firm, unqualified and unconditional offer to meet all the material terms of the ITB. Material terms are those that could affect the price, quantity, quality, or delivery. Also included as material terms are those which are clearly identified in the ITB, and which must be complied with at risk of bid rejection for non-responsiveness.

## **SECTION 2. SCOPE OF WORK AND CONTRACT INFORMATION**

### **SEC. 2.01 SCOPE OF WORK**

The Department of Family and Community Services, Office of Children’s Services (OCS) is soliciting bids from qualified vendors to result in a term contract for the printing and mailing of their confidential notifications.

#### **QUANTITIES:**

**THERE WILL BE DAILY MAILINGS ON EACH BUSINESS DAY, WITH AN ESTIMATED AMOUNT OF 70,000 LETTERS SENT ANNUALLY. THE 70,000 LETTERS WILL INCLUDE APPROXIMATELY 200,000 PAGES. OCS DOES NOT ANTICIPATE THERE WILL BE OVER 500 NOTICES TO BE MAILED PER DAY.**

#### **1. DESCRIPTION:**

Contractor will accept a confidential electronic file of PDFs from OCS to print, stuff into windowed envelopes, and mail within a 24-hour time period. There will be daily mailings on each business day, with an estimated amount of 70,000 letters sent annually. The 70,000 letters will include approximately 200,000 pages. OCS does not anticipate there will be over 500 notices to be mailed per day.

Contractor will work with OCS staff and the Department of Family and Community Services, Finance Management Services (FMS) staff to ensure compatibility of the two systems for the downloading of confidential PDF files. The contractor’s system will contain National Institute of Standards and Technology (NIST) compliant encryption protocols and will have File Transfer Protocol (FTP) connections with OCS.

#### **Processing**

Notices will be received from OCS in files that are PDF formatted. Addresses will be on the notices already. Notices will need to be printed in black ink on white text stock, 8.5” x 11”, 20#, tri-folded, stuffed into #10 window envelopes, posted and mailed within 24 hours of receiving the file from OCS. No special letterhead will be used.

Contractor will verify to OCS that the electronic file has been destroyed after printing.

Contractor will send OCS verification of # of notices received and # notices mailed.

Contractor will send invoices that detail number of notices and envelopes processed, number of pages processed.

Contractor will notify OCS well ahead of any upgrades.

File will be transmitted from the State to the vendor in a way that meets State and DFCS security guidelines, the file will be securely sent to the vendor’s secure drop site.

The vendor’s secure drop site must only be accessible by staff who are authorized to handle HIPAA data.

The method of printing the file must meet HIPAA standards.

#### **A. General**

\*\*\* Note: No Mailing List may be formed from these names and addresses, on notices or in address files, all names, addresses, and information contained in these notices and/or special mailings are confidential and may not be released by contractor, nor used for any purpose other than the administration of this contract. All client address files will be deleted after completion of printing.

**SECURITY:**

As the HIPAA protected health information will reside within the system, the winning vendor will be required to conform to and sign the attached Business Associate Agreement.

**ENCRYPTION OF DATA:** The vendor will be required to encrypt any State of Alaska information or data that is in use by the vendor both in transit and at rest at all times during the project and support after the project. This applies to any device that accesses State Data in any fashion. See previous section on “Sensitive Data and Encryption”.

**DESTRUCTION OF DATA:** When any vendor owned device that has had access to State Data is deemed to no longer require access to the State Data it must be cleaned and the data destroyed in compliance with the State and DFCS Security Policies.

**IT COMMUNICATION HIERARCHY:** After contract award, communication between the vendor and DFCS: All communications which may constitute a decision point for the project work must be documented in writing; includes change requests, project plan modifications, and deliverables.

**Support Communication:** Communication during the support period with the vendor will be limited to as-needed. Operational or business communications will be between the Vendor and the DFCS project manager or their designee.

## **2. STANDARDS FOR INFORMATION TECHNOLOGY (IT)**

Please see IT attachments A & F for standards of Information Technology as listed.

### **SEC. 2.02 CONTRACT TERM**

The initial term of the contract will be from March 1, 2025 through February 28, 2026 , with the option to renew for four (4) additional one-year terms under the same terms and conditions as the original contract. Renewals will be exercised at the sole discretion of the state.

Unless otherwise provided in this ITB, the State and the successful bidder/contractor agree: (1) that any extension of the contract excluding any exercised renewal options, will be considered as a month-to-month extension, and all other terms and conditions shall remain in full force and effect and (2) the procurement officer will provide notice to the contractor of the intent to cancel such month-to-month extension at least 30 days before the desired date of cancellation. A month-to-month extension may only be executed by the procurement officer via a written contract amendment.

### **SEC. 2.03 CONTRACT TYPE**

This contract is a Fixed-Firm contract.



**SEC. 2.04 PAYMENT FOR STATE PURCHASES**

No payment will be made until the contract is approved by the Commissioner of the Department of Family and Community Services or the Commissioner's designee. Under no conditions will the state be liable for the payment of any interest charges associated with the cost of the contract. The state is not responsible for and will not pay local, state, or federal taxes. All costs associated with the contract must be stated in U.S. currency.

Payment for agreements under \$500,000 for the undisputed purchase of goods or services provided to a state agency, will be made within 30 days of the receipt of a proper billing or the delivery of the goods or services to the location(s) specified in the agreement, whichever is later. A late payment is subject to 1.5% interest per month on the unpaid balance. Interest will not be paid if there is a dispute or if there is an agreement that establishes a lower interest rate or precludes the charging of interest.

**SEC. 2.05 ELECTRONIC PAYMENTS**

The State of Alaska prefers vendors receive payment via Electronic Funds Transfer (EFT). Bidders may review information concerning the EFT process and access the [Electronic Payment Agreement Form for Vendors](https://doa.alaska.gov/dof/vendor.html) at the following link: <https://doa.alaska.gov/dof/vendor.html>. Method of payment is not a factor in the State's determination for award.

Any single contract payments of \$1 million or higher must be accepted by the contractor via Electronic Funds Transfer (EFT).

**SEC. 2.06 PROMPT PAYMENT FOR STATE PURCHASES**

The state is eligible to receive a **5%** discount for all invoices paid within **15** business days from the date of receipt of the commodities or services and/or a correct invoice, whichever is later. The discount shall be taken on the full invoice amount. The state shall consider payment being made as either the date a printed warrant is issued or the date an electronic funds transfer (EFT) is initiated.

**SEC. 2.07 CONTRACT ADMINISTRATION**

The administration of this contract is the responsibility of the procurement officer or person appointed by the Department of Family and Community Services, Office of Children's Services.

**SEC. 2.08 CONTRACT PRICE ADJUSTMENTS**

A contract resulting from this ITB will include the following price adjustment clause:

**Consumer Price Index (CPI):** Contract prices will remain firm through 02/28/2026.

The Contractor or State may request price adjustments, no sooner than 12 months from the Contract execution date, and no more than once per contract year. Contractors must submit a request to the State at least thirty (30) days prior to the end of the current term. All Requests must be in writing and must be received 30 days prior to the Contract renewal date.

- a. If the Contractor or State fail to request a CPI price adjustment 30 days prior to the Contract renewal date, the adjustment will be effective 30 days after the State or Contractor receives their written request.
- b. Price adjustments will be made in accordance with the percentage change in the U.S. Department of Labor, Bureau of Labor and Statistics, Consumer Price Index (CPI-U) for All Urban Consumers, All Items, Urban Alaska.
- c. The price adjustment rate will be determined by comparing the percentage difference between the CPI in effect for the base year reported HALF1 (January through June 2023) (depends on the timing, may be HALF2 for July-December); and each HALF1 (or HALF2) thereafter. The percentage difference between those two CPI issues will be the price adjustment rate. No retroactive contract price adjustments will be allowed. All price adjustments must be approved by the Procurement Officer prior to the implementation of the adjusted pricing. Approval shall be in the form of a Contract Amendment issued by the Procurement Officer.
- d. Approval for all price increases is dependent upon full compliance with the terms of the Contract including reporting requirements.

## **SEC. 2.09 CONTRACT PERFORMANCE LOCATION**

The state **WILL NOT** provide workspace for the contractor. The contractor must provide its own workspace.

By signature on their bid, the bidder certifies that all services provided under this contract by the contractor and all subcontractors shall be performed in the United States.

If the bidder cannot certify that all work will be performed in the United States, the bidder must contact the procurement officer in writing to request a waiver at least 10 days prior to the deadline for receipt of bids.

The request must include a detailed description of the portion of work that will be performed outside the United States, where, by whom, and the reason the waiver is necessary.

Failure to comply with these requirements may cause the state to reject the bid as non-responsive or cancel the contract.

## **SEC. 2.10 THIRD-PARTY FINANCING AGREEMENTS NOT ALLOWED**

Because of the additional administrative and accounting time required of the state when third party financing agreements are permitted, they will not be allowed under this contract.

## **SEC. 2.11 SUBCONTRACTORS**

Subcontractors will not be allowed.

**SEC. 2.12 JOINT VENTURES**

Joint ventures will not be allowed.

**SEC. 2.13 RIGHT TO INSPECT PLACE OF BUSINESS**

At reasonable times, the state may inspect those areas of the contractor's place of business that are related to the performance of a contract. If the state makes such an inspection, the contractor must provide reasonable assistance.

**SEC. 2.14 F.O.B. POINT**

The F.O.B. point for all items purchased under this contract is the final destination anywhere within the State of Alaska. Ownership of and title to the ordered items remains with the contractor until the items have been delivered to their final destination and are accepted by the state.

The cost of shipping and delivery within all United States is to be included in the bid price. There will be no additional charge for shipping and delivery within the United States.

**SEC. 2.15 INSPECTION & MODIFICATION - REIMBURSEMENT FOR UNACCEPTABLE DELIVERABLES**

The contractor is responsible for providing all products or the completion of all work set out in the contract. All products or work is subject to inspection, evaluation, and approval by the state. The state may employ all reasonable means to ensure that the work is progressing and being performed in compliance with the contract. The state may instruct the contractor to make corrections or modifications if needed in order to accomplish the contract's intent. The contractor will not unreasonably withhold such changes.

Substantial failure of the contractor to perform the contract may cause the state to terminate the contract. In this event, the state may require the contractor to reimburse monies paid (based on the identified portion of unacceptable products or work received) and may seek associated damages.

**SEC. 2.16 EQUIPMENT INSPECTION**

Equipment offered (including for lease) may be subject to inspection and approval by the state prior to the award of the ITB. The equipment and attachments must be in good repair and capable of performing the work for which they were designed.

**SEC. 2.17 NEW EQUIPMENT**

Equipment offered in response to this ITB must be new equipment. New equipment means equipment that is currently in production by the manufacturer and is still the latest model, edition or version generally offered. The equipment must be warranted as new by the manufacturer and may not have been used for any purpose, other than display (not demonstration), prior to its sale to the state. The state will not accept remanufactured, used, or reconditioned equipment. It is the contractor's responsibility to ensure that each piece of equipment delivered to the state complies with this requirement. A contractor's failure to comply with this requirement will cause the state to seek remedies under breach of contract.

**SEC. 2.18 REMANUFACTURED/RECONDITIONED EQUIPMENT**

Remanufactured/reconditioned is acceptable provided it meets the requirements of this clause and the requirements of the rest of this ITB. Remanufactured/reconditioned equipment is defined as used equipment that has been remanufactured/ reconditioned and restored to new condition. All remanufactured/reconditioned equipment must have the same warranty as new equipment.

**SEC. 2.19 LEMON CLAUSE**

This clause applies to all equipment purchased through this contract. The application period is from the date of contract. This clause takes precedence over any other warranty or service maintenance clauses associated with this contract.

Any equipment that fails (except due to operator error) to operate according to the manufacturer's published performance specifications and/or is subject to recurring related problems must be replaced with the same make and model of new equipment at no cost to the state.

**SEC. 2.20 DISCONTINUED ITEMS**

In the event an item is discontinued by the manufacturer during the life of the contract, another item may be substituted, provided that the procurement officer makes a written determination that it is equal to or better than the discontinued item and provided that it is sold at the same price or less than the discontinued item.

**SEC. 2.21 SHIPPING DAMAGE**

The state will not accept or pay for damaged goods. The contractor must file all claims against the carrier(s) for damages incurred to items in transit from the point of origin to the ultimate destination. The state will provide the contractor with written notice when damaged goods are received. The state will deduct the cost of the damaged goods from the invoice prior to payment. The contractor must file all claims against the carrier(s) for reimbursement of the loss.

**SEC. 2.22 CONTRACT CHANGES – UNANTICIPATED AMENDMENTS**

During the course of this contract, the contractor may be required to perform additional work. That work will be within the general scope of the initial contract. When additional work is required, the state will provide the contractor a written description of the additional work and request the contractor to submit a firm time schedule for accomplishing the additional work and a firm price for the additional work. Cost and pricing data must be provided to justify the cost of such amendments per AS 36.30.400.

The contractor will not commence additional work until the procurement officer has secured required state approvals necessary and issued a written contract amendment.

**SEC. 2.23 CONTINUING OBLIGATION OF CONTRACTOR**

Notwithstanding the expiration date of a contract resulting from this ITB, the contractor is obligated to fulfill its responsibilities until warranty, guarantee, maintenance, and parts availability requirements have completely expired.

**SEC. 2.24 BILLING INSTRUCTIONS**

All invoices produced by the contractor must contain the following information at a minimum:

1. Vendor remit to address
2. Contract number
3. Invoice number
4. Invoice date
5. List of Services rendered

Invoices must be billed to the ordering agency's address shown on the individual Purchase Order, Contract Award or Delivery Order. The state will make payment after it receives the goods or services and the invoice. Questions concerning payment must be addressed to the ordering agency.

**SEC. 2.25 ESTIMATED QUANTITIES**

The quantities referenced in this ITB are estimated requirements and may vary more or less from the quantities actually purchased. The State does not guarantee any minimum or maximum purchase. Orders will be issued throughout the contract period on an as-needed basis.

**SEC. 2.26 NONDISCLOSURE AND CONFIDENTIALITY**

Contractor agrees that all confidential information shall be used only for purposes of providing the deliverables and performing the services specified herein and shall not disseminate or allow dissemination of confidential information except as provided for in this section. The contractor shall hold as confidential and will use reasonable care (including both facility physical security and electronic security) to prevent unauthorized access by, storage, disclosure, publication, dissemination to and/or use by third parties of, the confidential information. "Reasonable care" means compliance by the contractor with all applicable federal and state law, including the Social Security Act and HIPAA. The contractor must promptly notify the state in writing if it becomes aware of any storage, disclosure, loss, unauthorized access to or use of the confidential information.

Confidential information, as used herein, means any data, files, software, information or materials (whether prepared by the state or its agents or advisors) in oral, electronic, tangible or intangible form and however stored, compiled or memorialized that is classified confidential as defined by State of Alaska classification and categorization guidelines provided by the state to the contractor or a contractor agent or otherwise made available to the contractor or a contractor agent in connection with this contract, or acquired, obtained or learned by the contractor or a contractor agent in the performance of this contract. Examples of confidential information include, but are not limited to technology infrastructure, architecture, financial data, trade secrets, equipment specifications, user lists, passwords, research data, and technology data (infrastructure, architecture, operating systems, security tools, IP addresses, etc.).

If confidential information is requested to be disclosed by the contractor pursuant to a request received by a third party and such disclosure of the confidential information is required under applicable state or federal law, regulation, governmental or regulatory authority, the contractor may disclose the confidential information after providing the state with written notice of the requested disclosure ( to the extent such notice to the state is permitted by applicable law) and giving the state opportunity to review the request. If the contractor receives no

objection from the state, it may release the confidential information within 30 days. Notice of the requested disclosure of confidential information by the contractor must be provided to the state within a reasonable time after the contractor's receipt of notice of the requested disclosure and, upon request of the state, shall seek to obtain legal protection from the release of the confidential information.

The following information shall not be considered confidential information: information previously known to be public information when received from the other party; information freely available to the general public; information which now is or hereafter becomes publicly known by other than a breach of confidentiality hereof; or information which is disclosed by a party pursuant to subpoena or other legal process and which as a result becomes lawfully obtainable by the general public.

## **SEC. 2.27 INDEMNIFICATION**

The contractor shall indemnify, hold harmless, and defend the contracting agency from and against any claim of, or liability for error, omission or negligent act of the contractor under this agreement. The contractor shall not be required to indemnify the contracting agency for a claim of, or liability for, the independent negligence of the contracting agency. If there is a claim of, or liability for, the joint negligent error or omission of the contractor and the independent negligence of the contracting agency, the indemnification and hold harmless obligation shall be apportioned on a comparative fault basis.

“Contractor” and “contracting agency”, as used within this and the following article, include the employees, agents and other contractors who are directly responsible, respectively, to each. The term “independent negligence” is negligence other than in the contracting agency's selection, administration, monitoring, or controlling of the contractor and in approving or accepting the contractor's work.

## **SEC. 2.28 INSURANCE**

Without limiting the contractor's indemnification, it is agreed that the contractor shall purchase at its own expense and maintain in force at all times during the performance of services under this agreement the following policies of insurance. Where specific limits are shown, it is understood that they shall be the minimum acceptable limits. If the contractor's policy contains higher limits, the state shall be entitled to coverage to the extent of such higher limits.

Certificates of Insurance must be furnished to the procurement officer prior to contract approval and must provide for a notice of cancellation, non-renewal, or material change of conditions in accordance with policy provisions. Failure to furnish satisfactory evidence of insurance or lapse of the policy is a material breach of this contract and shall be grounds for termination of the contractor's services. All insurance policies shall comply with and be issued by insurers licensed to transact the business of insurance under AS 21.

### **Proof of insurance is required for the following:**

- Workers' Compensation Insurance: The contractor shall provide and maintain, for all employees engaged in work under this contract, coverage as required by AS 23.30.045, and where applicable, any other statutory obligations including but not limited to Federal U.S.L. & H. and Jones Act requirements. The policy must waive subrogation against the state.

- Commercial General Liability Insurance: covering all business premises and operations used by the contractor in the performance of services under this agreement with minimum coverage limits of \$300,000 combined single limit per occurrence.
- Commercial Automobile Liability Insurance: covering all vehicles used by the contractor in the performance of services under this agreement with minimum coverage limits of \$300,000 combined single limit per occurrence.

## **SECTION 3. BID FORMAT AND CONTENT**

### **SEC. 3.01 BID FORMS**

Bidders shall use the front page of this ITB, the Bid Submission Cover Sheet, and any other forms identified in this ITB for submitting bids. All bids must be signed by an individual authorized to bind the bidder to the provisions of the ITB.

#### **BIDDER'S CERTIFICATION**

By signature on the bid, the bidder certifies that they comply with the following:

- A. the laws of the State of Alaska;
- B. the applicable portion of the Federal Civil Rights Act of 1964;
- C. the Equal Employment Opportunity Act and the regulations issued thereunder by the state and federal government;
- D. the Americans with Disabilities Act of 1990 and the regulations issued thereunder by the state and federal government and certifies that programs, services, and activities provided to the general public on behalf of the State under a contract resulting from this solicitation comply with the Americans with Disabilities Act of 1990, 28 CFR, Part 35, Subpart B 35.130;
- E. all terms and conditions set out in this ITB;
- F. the price(s) submitted was arrived at independently arrived and without collusion, under penalty of perjury; and
- G. that the bid will remain open and valid for at least 90 days.

If any bidder fails to comply with [a] through [g] of this paragraph, the state reserves the right to disregard the bid, terminate the contract, or consider the contractor in default.

#### **CONFLICT OF INTEREST**

Each bid shall include a statement indicating whether the company or any individuals working on the contract has a possible conflict of interest (e.g., currently employed by the State of Alaska or formerly employed by the State of Alaska within the past two years) and, if so, the nature of that conflict. The procurement officer reserves the right to **consider a bid non-responsive and reject it** or cancel the award if any interest disclosed from any source could either give the appearance of a conflict or cause speculation as to the objectivity of the contract to be performed by the bidder.

### **SEC. 3.02 PRICES**

The bidder shall state prices in the units of issue on this ITB. Prices quoted in bids must be exclusive of federal, state, and local taxes. If the bidder believes that certain taxes are payable by the state, the bidder may list such taxes separately, directly below the bid price for the affected item.



## SECTION 4. EVALUATION AND CONTRACTOR SELECTION

### SEC. 4.01 EVALUATION OF BIDS

After bid opening, the procurement officer will evaluate the bids for responsiveness. Bids deemed non-responsive will be eliminated from further consideration. An evaluation may not be based on discrimination due the race, religion, color, national origin, sex, age, marital status, pregnancy, parenthood, disability, or political affiliation of the bidder.

### SEC. 4.02 APPLICATION OF PREFERENCES

Certain preferences apply to all state contracts, regardless of their dollar value. The Alaska Bidder and Alaska Veteran preferences are the most common preferences involved in the ITB process. Additional preferences that may apply to this procurement are listed below. Guides that contain excerpts from the relevant statutes and codes, explain when the preferences apply and provide examples of how to calculate the preferences are available at the following website:

<https://oppm.doa.alaska.gov/policy-oversight/policy-resources/user-guide-matrixes/>

- Alaska Military Skills Program Preference – AS 36.30.321(I)
- Alaska Products Preference - AS 36.30.332
- Recycled Products Preference - AS 36.30.337
- Local Agriculture and Fisheries Products Preference - AS 36.15.050
- Employment Program Preference - AS 36.30.321(b)
- Alaskans with Disabilities Preference - AS 36.30.321(d)

The Division of Vocational Rehabilitation in the Department of Labor and Workforce Development keeps a list of qualified employment programs and individuals who qualify as persons with a disability. As evidence of a business' or an individual's right to the Employment Program or Alaskans with Disabilities preferences, the Division of Vocational Rehabilitation will issue a certification letter. To take advantage of these preferences, a business or individual must be on the appropriate Division of Vocational Rehabilitation list prior to the time designated for receipt of proposals. Bidders must attach a copy of their certification letter to the proposal. **A bidder's failure to provide this certification letter with their proposal will cause the state to disallow the preference.**

### SEC. 4.03 ALASKA BIDDER PREFERENCE

An Alaska Bidder Preference of 5% will be applied to the total bid price. The preference will be given to a bidder who:

- 1) holds a current Alaska business license prior to the deadline for receipt of bids;
- 2) submits a bid for goods or services under the name appearing on the bidder's current Alaska business license;

- 3) has maintained a place of business within the state staffed by the bidder, or an employee of the bidder, for a period of six months immediately preceding the date of the bid;
- 4) is incorporated or qualified to do business under the laws of the state, is a sole proprietorship and the proprietor is a resident of the state, is a limited liability company (LLC) organized under AS 10.50 and all members are residents of the state, or is a partnership under AS 32.06 or AS 32.11 and all partners are residents of the state; and
- 5) if a joint venture, is composed entirely of ventures that qualify under (1)-(4) of this subsection.

**Alaska Bidder Preference Certification Form**

To receive the Alaska Bidder Preference, the bid must include the Alaska Bidder Preference Certification Form attached to this ITB. A bidder does not need to complete the Alaska Veteran Preference questions on the form if not claiming the Alaska Veteran Preference. A bidder's failure to provide this completed form with their bid will cause the state to disallow the preference.

**SEC. 4.04 ALASKA VETERAN PREFERENCE**

An Alaska Veteran Preference of 5%, not to exceed \$5,000, will be applied to the total bid price. The preference will be given to a bidder who qualifies under AS 36.30.990(2) as an Alaska Bidder and is a:

- a) sole proprietorship owned by an Alaska veteran;
- b) partnership under AS 32.06 or AS 32.11 if a majority of the partners are Alaska veterans;
- c) limited liability company organized under AS 10.50 if a majority of the members are Alaska veterans; or
- d) corporation that is wholly owned by individuals, and a majority of the individuals are Alaska veterans.

In accordance with AS 36.30.321(i), the bidder must also add value by actually performing, controlling, managing, and supervising the services provided, or for supplies, the bidder must have sold supplies of the general nature solicited to other state agencies, other government, or the general public.

**Alaska Veteran Preference Certification**

To receive the Alaska Veteran Preference, the bid must include the Alaska Bidder Preference Certification Form attached to this ITB. A bidder's failure to provide this completed form with their bid will cause the state to disallow the preference.

**SEC. 4.05 ALASKA MILITARY SKILLS PROGRAM PREFERENCE**

An Alaska Military Skills Program Preference of 2%, not to exceed \$5,000, will be applied to the price in the proposal. The preference will be given to an offeror who qualifies under AS 36.30.990(2) as an Alaska bidder and:

- a) Employs at least one person who is currently enrolled in, or within the previous two years graduated from, a United States Department of Defense SkillBridge or United States Army career skills program for service members or spouses of service members that offers civilian work experience through specific industry training, pre-apprenticeships, registered apprenticeships, or internships during the last 180 days before a service member separates or retires from the service; or
- b) has an active partnership with an entity that employs an apprentice through a program described above.

In accordance with AS 36.30.321(i), the bidder must also add value by actually performing, controlling, managing, and supervising the services provided, or for supplies, the bidder must have sold supplies of the general nature solicited to other state agencies, other government, or the general public.

#### **Alaska Military Skills Program Preference Certification**

In order to receive the Alaska Military Skills Program Preference, the bid must include the Alaska Bidder Preference Certification Form attached to this ITB. A bidder's failure to provide this completed form with their bid will cause the state to disallow the preference.

In addition, proof of graduation of the qualifying employee from an eligible program as described in AS 36.30.321(l) must be provided to the Procurement Officer at time of bid submission. Bidders must provide clarification or additional information requested by the Procurement Officer related to the preference not later than 5:00 PM Alaska Time one (1) business day following the date of the request. Failure to provide sufficient documentation will result in the bidder not receiving the Military Skills Program Preference.

### **SEC. 4.06 USE OF LOCAL FOREST PRODUCTS**

In a project financed by state money in which the use of timber, lumber and manufactured lumber is required, only timber, lumber and manufactured lumber products originating in this state from Alaska forests shall be used unless the use of those products has been determined to be impractical, in accordance with AS 36.15.010 and AS 36.30.322.

### **SEC. 4.07 LOCAL AGRICULTURAL AND FISHERIES PRODUCT PREFERENCE**

When agricultural, dairy, timber, lumber, or fisheries products are purchased using state money, a seven percent (7%) preference shall be applied to the price of the products harvested in Alaska, or in the case of fisheries products, the products harvested or processed within the jurisdiction of Alaska, in accordance with AS 36.15.050.

### **SEC. 4.08 ALASKA PRODUCT PREFERENCE**

A bidder that designates the use of an Alaska Product which meets the requirements of the ITB specifications and is designated as a Class I, Class II, or Class III Alaska Product by the Department of Community & Economic Development (DCCED) may receive a preference in the bid evaluation in accordance with AS 36.30.332 and 3 AAC 92.010.

To qualify for the preference, the product must have received certification from DCCED, be listed in the current published edition of the Alaska Products Preference List, and the bidder must provide the qualified product on a 100% basis. There are no provisions under Alaska Statutes or Regulations that allow for a product exchanges/substitutions or permit the product to be co-mingled with other products. Rather, AS 36.30.330 provides for a penalty for failing to use the designated Alaska products.

Products are classified in one of three categories:

- Class I products receive a 3% preference.
- Class II products receive a 5% preference.
- Class III products receive a 7% preference.

When the bids are evaluated, the preference percentage will be deducted from the product price. If a bidder fails to specify the brand being offered, no preference will be given. For more information on the Alaska Product Preference and to see the list of products currently on the Alaska Product Preference List, use the following web link:

<https://www.commerce.alaska.gov/web/dcra/AlaskaProductPreferenceProgram.aspx>

**Brand Offered**

If offering a product that qualifies for the Alaska Product Preference, the bidder must indicate the brand of product they intent to provide. If a bidder is not offering a product that qualifies for the Alaska Product Preference, the bidder does not need to indicate a product brand.

**Brand of Product Changes**

During the course of the contract including all renewal options, a contractor that offered a product that qualified for the Alaska Product Preference wishes to change the product brand, the contractor must first provide a written request, along with evidence that the replacement brand also qualifies for the Alaska Product Preference, for approval by the procurement officer. A contract amendment must be issued by the procurement officer to authorize the change.

If a bidder offers a product brand in the original bid that does not qualify for the Alaska Product Preference, a change in the product brand may be made at any time during the course of the contract, including all renewals, as long as the product band continues to meet the required specifications. A contract amendment is not required if the product brand originally offered did not qualify for the Alaska Product Preference.

**SEC. 4.09 EMPLOYMENT PROGRAM PREFERENCE**

If a bidder qualifies for the Alaska Bidder Preference and is offering goods or services through an employment program as defined under AS 36.30.990(12), an Employment Program Preference of 15% will be applied to the total bid price.

In accordance with AS 36.30.321(i), the bidder must also add value by actually performing, controlling, managing, and supervising the services provided, or for supplies, the bidder must have sold supplies of the general nature solicited to other state agencies, other government, or the general public.

**SEC. 4.10 ALASKANS WITH DISABILITIES PREFERENCE**

If a bidder qualifies for the Alaska Bidder Preference and is a qualifying entity as defined in AS 36.30.321(d), an Alaskans with Disabilities Preference of 10% will be applied to the total bid price.

In accordance with AS 36.30.321(i), the bidder must also add value by actually performing, controlling, managing, and supervising the services provided, or for supplies, the bidder must have sold supplies of the general nature solicited to other state agencies, other government, or the general public.

**SEC. 4.11 PREFERENCE QUALIFICATION LETTER**

Regarding the Employment Program Preference and the Alaskans with Disabilities Preference, the Division of Vocational Rehabilitation in the Department of Labor and Workforce Development maintains lists companies who qualify for those preferences. As evidence of a company's right to the preferences, the Division of Vocational Rehabilitation will issue a certification letter. To take advantage of the preferences, a bidder must be on the appropriate Division of Vocational Rehabilitation list at the time the bid is opened and must attach a copy of their certification letter to their bid. The bidder's failure to provide this certification letter with their bid will cause the state to disallow the preference.

**SEC. 4.12 EXTENSION OF PRICES**

In case of error in the extension of prices in the bid, the unit prices will govern; in a lot bid, the lot prices will govern.

**SEC. 4.13 METHOD OF AWARD**

Award will be made to the lowest responsive and responsible bidder. To be considered responsive, bidders must bid on all items.

**SEC. 4.14 CONTRACTOR SELECTION PROCESS**

Once the contracts are established this selection process will be used. When the state needs to order the product or service, the lowest priced contractor for that location will be contacted first. If, for any reason, the lowest contractor is not available to perform the needed service, the state will contact the next lowest priced contractor for that location. This process will continue until a contractor who can perform the service is located. The location of the contractor initially contacted will be determined by the starting location of the call-out. For example, if a there was a need to transport a person from Anchorage to Fairbanks and then guard the person for two days in Fairbanks, the agency would contact Anchorage contractors, even though a substantial portion of the actual service would be performed in Fairbanks.

**SEC. 4.15 NOTICE OF INTENT TO AWARD**

After the responses to this ITB have been opened and evaluated, a tabulation of the bids will be prepared. This tabulation, called a Notice of Intent to Award, serves two purposes. It lists the name of each company or person that offered a bid and the price they bid. It also provides notice of the state's intent to award a contract(s) to the bidder(s) indicated. A copy of the Notice of Intent will be sent to each company or person who responded to the ITB. Bidders identified as the apparent low responsive bidders are instructed not to proceed until a Purchase Order, Contract Award, Lease, or some other form of written notice is given by the procurement officer. A company or person who proceeds prior to receiving a Purchase Order, Contract Award, Lease, or some other form of written notice from the procurement officer does so without a contract and at their own risk.

## **SECTION 5. GENERAL PROCESS AND LEGAL INFORMATION**

### **SEC. 5.01 INFORMAL DEBRIEFING**

When the contract is completed, an informal debriefing may be performed at the discretion of the procurement officer. If performed, the scope of the debriefing will be limited to the products provided or work performed by the contractor.

### **SEC. 5.02 ALASKA BUSINESS LICENSE AND OTHER REQUIRED LICENSES**

Prior to the award of a contract, a bidder must hold a valid Alaska business license. However, to receive the Alaska Bidder Preference and other related preferences, such as the Alaska Veteran Preference and Alaskans with Disabilities Preference, a bidder must hold a valid Alaska business license prior to the deadline for receipt of bids. Bidders should contact the **Department of Commerce, Community and Economic Development, Division of Corporations, Business, and Professional Licensing, PO Box 110806, Juneau, Alaska 99811-0806**, for information on these licenses. Acceptable evidence that the bidder possesses a valid Alaska business license may consist of any one of the following:

- copy of an Alaska business license,
- certification on the bid that the bidder has a valid Alaska business license and has included the license number in the bid,
- a canceled check for the Alaska business license fee,
- a copy of the Alaska business license application with a receipt stamp from the state's occupational licensing office, or
- a sworn and notarized statement that the bidder has applied and paid for the Alaska business license.

You are not required to hold a valid Alaska business license at the time bids are opened if you possess one of the following licenses and are offering services or supplies under that specific line of business:

- fisheries business licenses issued by Alaska Department of Revenue or Alaska Department of Fish and Game,
- liquor licenses issued by Alaska Department of Revenue for alcohol sales only,
- insurance licenses issued by Alaska Department of Commerce, Community and Economic Development, Division of Insurance, or
- Mining licenses issued by Alaska Department of Revenue.

Prior the deadline for receipt of bids, all bidders must hold any other necessary applicable professional licenses required by Alaska Statute.

### **SEC. 5.03 AUTHORITY**

This ITB is written in accordance with AS 36.30 and 2 AAC 12.

**SEC. 5.04 COMPLIANCE**

In the performance of a contract that results from this ITB, the contractor must comply with all applicable federal, state, and borough regulations, codes, and laws; be liable for all required insurance, licenses, permits and bonds; and pay all applicable federal, state, and borough taxes.

**SEC. 5.05 SUITABLE MATERIALS, ETC.**

Unless otherwise specified in this ITB, all materials, supplies or equipment offered by a bidder shall be new, unused, and of the latest edition, version, model, or crop and of recent manufacture.

**SEC. 5.06 SPECIFICATIONS**

Unless otherwise specified in this ITB, product brand names or model numbers specified in this ITB are examples of the type and quality of product required and are not statements of preference. If the specifications describing an item conflict with a brand name or model number describing the item, the specifications govern. Reference to brand name or number does not preclude an offer of a comparable or better product, if full specifications and descriptive literature are provided for the product. Failure to provide such specifications and descriptive literature may be cause for rejection of the offer.

**SEC. 5.07 BRAND SPECIFIC**

Certain items may be designated brand specific. When an item is designated no substitutions for the brand and model specified will be allowed.

**SEC. 5.08 ITEM UPGRADES**

The state reserves the right to accept upgrades to models on the basic contract when the upgrades improve the way the equipment operates or improve the accuracy of the equipment. Such upgraded items must be at the same price as the items in the basic contract.

**SEC. 5.09 CONTRACTOR SITE INSPECTION**

The state may conduct on-site visits to evaluate the bidder's capacity to perform the contract. A bidder must agree, at risk of being found non-responsive and having its bid rejected, to provide the state reasonable access to relevant portions of its work sites. Individuals designated by the procurement officer at the state's expense will make site inspection.

**SEC. 5.10 ORDER DOCUMENTS**

Except as specifically allowed under this ITB, an ordering agency will not sign any vendor contract. The state is not bound by a vendor contract signed by a person who is not specifically authorized to sign for the state under this ITB. Unless otherwise specified in this ITB, the State of Alaska Purchase Order, Contract Award and Delivery Order are the only order documents that may be used to place orders against the contract(s) resulting from this ITB.

**SEC. 5.11 HUMAN TRAFFICKING**

By signature on their bid, the bidder certifies that the bidder is not established and headquartered or incorporated and headquartered in a country recognized as Tier 3 in the most recent United States Department of State's Trafficking in Persons Report.

The most recent United States Department of State's Trafficking in Persons Report can be found at the following website: <http://www.state.gov/j/tip/>

Failure to comply with this requirement will cause the state to reject the bid as non-responsive or cancel the contract.

**SEC. 5.12 RIGHT OF REJECTION**

Bidders must comply with all the terms of the ITB, the State Procurement Code (AS 36.30), and all applicable local, state, and federal laws, codes, and regulations. The procurement officer may reject any bid that does not comply with all the material and substantial terms, conditions, and performance requirements of the ITB.

Bidders may not qualify the bid nor restrict the rights of the state. If a bidder does so, the procurement officer may determine the bid to be a non-responsive counteroffer, and the bid may be rejected.

Minor informalities that:

- do not affect responsiveness,
- are merely a matter of form or format,
- do not change the relative standing or otherwise prejudice other bidders,
- do not change the meaning or scope of the ITB,
- are trivial, negligible, or immaterial in nature,
- do not reflect a material change in the work, or
- do not constitute a substantial reservation against a requirement or provision,

may be waived by the procurement officer.

The state reserves the right to refrain from making an award if it is determined to be in the state's best interest. **A bid from a debarred or suspended bidder shall be rejected.**

**SEC. 5.13 STATE NOT RESPONSIBLE FOR PREPARATION COSTS**

The state will not pay any cost associated with the preparation, submittal, presentation, or evaluation of any bid.



**SEC. 5.14 DISCLOSURE OF BID CONTENTS**

All bid prices become public information at the bid opening. After the deadline for receipt of bids, all other bid material submitted become the property of the State of Alaska and may be returned only at the state's option. AS 40.25.110 requires public records to be open to reasonable inspection. All other bid information will be held in confidence during the evaluation process and prior to the time a Notice of Intent to Award is issued. Thereafter, bids will become public information.

The Office of Procurement and Property Management (OPPM), or their designee recognizes that some information a bidder submits might be confidential under the United States or the State of Alaska Constitution, a federal statute or regulation, or a State of Alaska statute: i.e., might be confidential business information (CBI). *See, e.g.*, article 1, section 1 of the Alaska Constitution; AS 45.50.910 – 45.50.945 (the Alaska Uniform Trade Secrets Act); *DNR v. Arctic Slope Regional Corp.*, 834 P.2d 134, 137-39 (Alaska 1991). For OPPM or their designee to treat information a bidder submits with its bid as CBI, the bidder must do the following when submitting their bid: (1) mark the specific information it asserts is CBI; and (2) for each discrete set of such information, identify, in writing, each authority the bidder asserts make the information CBI. If the bidder does not do these things, the information will become public after the Notice of Intent to Award is issued. If the bidder does these things, OPPM or their designee will evaluate the bidder's assertion upon receiving a request for the information. If OPPM or their designee reject the assertion, they will, to the extent permitted by federal and State of Alaska law, undertake reasonable measures to give the bidder an opportunity to object to the disclosure of the information.

**SEC. 5.15 ASSIGNMENTS**

Per 2 AAC 12.480, the contractor may not transfer or assign any portion of the contract without prior written approval from the procurement officer. Bids that are conditioned upon the state's approval of an assignment will be rejected as non-responsive.

**SEC. 5.16 FORCE MAJEURE (IMPOSSIBILITY TO PERFORM)**

The parties to a contract resulting from this ITB are not liable for the consequences of any failure to perform, or default in performing, any of its obligations under the contract, if that failure or default is caused by any unforeseeable Force Majeure, beyond the control of, and without the fault or negligence of, the respective party.

For the purposes of this ITB, Force Majeure will mean war (whether declared or not); revolution; invasion; insurrection; riot; civil commotion; sabotage; military or usurped power; lightning; explosion; fire; storm; drought; flood; earthquake; epidemic; quarantine; strikes; acts or restraints of governmental authorities affecting the project or directly or indirectly prohibiting or restricting the furnishing or use of materials or labor required; inability to secure materials, machinery, equipment or labor because of priority, allocation or other regulations of any governmental authorities.

**SEC. 5.17 DEFAULT**

In case of default by the contractor, for any reason whatsoever, the state may procure the goods or services from another source and hold the contractor responsible for any resulting excess cost and may seek other remedies under law or equity.

**SEC. 5.18 DISPUTES**

If the contractor has a claim arising in connection with the contract that it cannot resolve with the state by mutual agreement, it shall pursue the claim, if at all, in accordance with the provisions of AS 36.30.620 – AS 36.30.632.

**SEC. 5.19 SEVERABILITY**

If any provision of the contract or agreement is found to be invalid or declared by a court to be illegal or in conflict with any law, the validity of the remaining terms and provisions will not be affected; and the rights and obligations of the parties will be construed and enforced as if the contract did not contain the particular provision held to be invalid.

**SEC. 5.20 CONTRACT CANCELLATION**

- 1) The state reserves the right to cancel the contract at its convenience upon thirty (30) calendar days written notice to the contractor. The state is only liable for payment in accordance with the payment provisions of this contract for supplies or services provide before the effective date termination.
- 2) By signature on their bid, the bidder certifies that they will not support or participate in a boycott of the State of Israel. Failure to comply with this requirement may cause the state to reject the bid as non-responsive or cancel the contract.

**SEC. 5.21 GOVERNING LAW; FORUM SELECTION**

A contract resulting from this ITB is governed by the laws of the State of Alaska. To the extent not otherwise governed by Section 5.15 of this ITB, any claim concerning the contract shall be brought only in the Superior Court of the State of Alaska and not elsewhere.

**SEC. 5.22 QUALIFIED BIDDERS**

Per 2 AAC 12.875, unless provided for otherwise in the ITB, to qualify as a bidder for award of a contract issued under AS 36.30, the bidder must:

- 1) Add value in the contract by actually performing, controlling, managing, or supervising the services to be provided; or
- 2) Be in the business of selling and have actually sold on a regular basis the supplies that are the subject of the ITB.

If the bidder leases services or supplies or acts as a broker or agency in providing the services or supplies to meet these requirements, the procurement officer may not accept the bidder as a qualified bidder under AS 36.30.

**SEC. 5.23 FEDERALLY IMPOSED TARIFFS**

Changes in price (increase or decrease) resulting directly from a new or updated federal tariff, excise tax, or duty, imposed after contract award may be adjusted during the contract period or before delivery into the United States via contract amendment.

- **Notification of Changes:** The contractor must promptly notify the procurement officer in writing of any new, increased, or decreased federal excise tax or duty that may result in either an increase or decrease in the contract price and shall take appropriate action as directed by the procurement officer.
- **After-imposed or Increased Taxes and Duties:** Any federal excise tax or duty for goods or services covered by this contract that was exempted or excluded on the contract award date but later imposed on the contractor during the contract period, as the result of legislative, judicial, or administrative action may result in a price increase provided:
  - a) The tax or duty takes effect after the contract award date and isn't otherwise addressed by the contract.
  - b) The contractor warrants, in writing, that no amount of the newly imposed federal excise tax or duty or rate increase was included in the contract price, as a contingency or otherwise.
- **After-relieved or Decreased Taxes and Duties:** The contract price shall be decreased by the amount of any decrease in federal excise tax or duty for goods or services under the contract, except social security or other employment [taxes](#), that the contractor is required to pay or bear, or does not obtain a refund of, through the contractor's fault, negligence, or failure to follow instructions of the procurement officer.
- **State's Ability to Make Changes:** The state reserves the right to request verification of federal excise tax or duty amounts on goods or services covered by this contract and increase or decrease the contract price accordingly.
- **Price Change Threshold:** No adjustment shall be made in the contract price under this clause unless the amount of the adjustment exceeds \$250.

## **SEC. 5.24 PROTEST**

AS 36.30.560 provides that an interested party may protest the content of the ITB.

An interested party is defined in 2 AAC 12.990(a) (7) as "an actual or prospective bidder or bidder whose economic interest might be affected substantially and directly by the issuance of a contract solicitation, the award of a contract, or the failure to award a contract."

If an interested party wishes to protest the content of a solicitation, the protest must be received, in writing, by the procurement officer at least ten days prior to the deadline for receipt of bids.

AS 36.30.560 also provides that an interested party may protest the award of a contract or the proposed award of a contract.

If a bidder wishes to protest the award of a contract or the proposed award of a contract, the protest must be received, in writing, by the procurement officer within ten days after the date the Notice of Intent to Award the contract is issued.

A protester must have submitted a bid to have sufficient standing to protest the proposed award of a contract. Protests must include the following information:

- the name, address, and telephone number of the protester,
- the signature of the protester or the protester's representative,
- identification of the contracting agency and the solicitation or contract at issue,
- a detailed statement of the legal and factual grounds of the protest including copies of relevant documents, and
- the form of relief requested.

Protests filed by telex or telegram are not acceptable because they do not contain a signature. Fax copies containing a signature are acceptable.

The procurement officer will issue a written response to the protest. The response will set out the procurement officer's decision and contain the basis of the decision within the statutory time limit in AS 36.30.580. A copy of the decision will be furnished to the protester by certified mail, fax or another method that provides evidence of receipt.

All bidders will be notified of any protest. The review of protests, decisions of the procurement officer, appeals, and hearings, will be conducted in accordance with the State Procurement Code (AS 36.30), Article 8 "Legal and Contractual Remedies."

## **SECTION 6. ATTACHMENTS**

### **SEC. 6.01 ATTACHMENTS**

**Attachments:**

- 1) Bidder Preference Certification Forms
- 2) Bid Schedule
- 3) DFCS IT Requirements
- 4) DFCS Data Destruction Information and References



## ALASKA BIDDER PREFERENCE CERTIFICATION FORM AS 36.30.321 (A) / AS 36.30.990 (2)

<b>Solicitation Number</b>	
<b>Project Description</b>	
<b>Business Name</b>	
<b>Alaska Business License Number</b>	

A signed copy of this form must be included with your bid or proposal no later than the deadline set for receipt of bids or proposals.

If you are submitting a bid or proposal as a **JOINT VENTURE**, all members of the joint venture must complete and submit this form before the deadline set for receipt of bids or proposals. [AS 36.30.990\(2\)\(E\)](#)

**If the procuring agency is unable to verify a response, the preference may not be applied.** Knowingly or intentionally making false or misleading statements on this form, whether it succeeds in deceiving or misleading, constitutes misrepresentation per [AS 36.30.687](#) and may result in criminal penalties.

### **SIGNATURE**

By signature below, I certify under penalty of law that I am an authorized representative of the above entity and all information on this form is true and correct to the best of my knowledge.

<b>Printed Name:</b>	
<b>Title:</b>	
<b>Date:</b>	
<b>Signature:</b>	

<b>Alaska Bidder Preference:</b> Do you believe your firm qualifies for the Alaska Bidder Preference?	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Alaska Veterans Preference:</b> Do you believe your firm qualifies for the Alaska Veteran Preference?	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Alaska Military Skills Program Preference:</b> Do you believe your firm qualifies for the Alaska Military Skills Program Preference?	<input type="checkbox"/> Yes <input type="checkbox"/> No

To qualify for and claim the **Alaska Bidder Preference** you must answer **YES** to all questions in the Alaska Bidder Preference Question section below:

### Alaska Bidder Preference Questions

1	Does your business hold a current Alaska business license per AS 36.30.990(2)(A)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
2	Is your business submitting a bid or proposal under the name appearing on the Alaska Business license identified above? Per AS36.30.990 (2)(B)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
3	Has your business maintained a place of business within the state staffed by the bidder or offeror or an employee of the bidder or offeror for a period of six months immediately preceding the date of the bid or proposal per AS 36.30.990 (2)(C)?	<input type="checkbox"/> Yes <input type="checkbox"/> No

If the answer to question 3 is YES, complete the following:

<b>Physical Place of Business Address</b>	
<b>City</b>	
<b>Zip Code</b>	

“Place of business” is defined as a location at which normal business activities are conducted, services are rendered, or goods are made, stored, or processed; a post office box, mail drop, telephone, or answering service does not, by itself, constitute a place of business per [2 AAC 12.990\(b\)\(3\)](#).

Do you certify the Place of Business identified above meets this definition?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

**Per AS 16.05.415(a) per 2AAC 12.990(b)(7), the bidder or offeror, or at least one employee of the bidder or offeror must be a resident of the state?**

1	Do you certify the bidder or offeror, or, at least one employee of the bidder or offeror is physically present in the state with the intent to remain in Alaska indefinitely and to make a home in the state per AS 16.05.415(a)(2)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
2	Do you certify the resident(s) used to meet this requirement has maintained a domicile in Alaska for the 12 months immediately preceding the deadline set for receipt of bids or proposals per AS 16.05.415(a)(2)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
3	Do you certify the resident(s) used to meet this requirement is only claiming residency in Alaska per AS 16.05.415(a)(3)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
4	Do you certify the resident used to meet this requirement is not obtaining benefits under a claim of residency in another state, territory, or country per As 16.05.415 (a)(4)?	<input type="checkbox"/> Yes <input type="checkbox"/> No

**Per AS 36.30.990(2)(D), is your business:**

1	Incorporated or qualified to do business under the laws of the state?	<input type="checkbox"/> Yes <input type="checkbox"/> No
---	---	--

**If yes, enter the current Alaska Corporate Entity Number:**

**Indicate below how your business is organized:**

1	Is your business a Sole Proprietorship and the Proprietor is a resident of the state?	<input type="checkbox"/> Yes <input type="checkbox"/> No
2	Is your business a Limited Liability Corporation organized under AS 10.50 and <b>ALL</b> members are residents of the state?	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>If the answer to question 2 above is YES, please identify each member by name:</b>		
3	Is your business a partnership under former AS32.05, AS32.06, or AS32.11 and all partners are residents of the state?	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>If the answer to question 3 above is YES, please identify each partner by name:</b>		

---



**Alaska Veterans Preference Questions:**

To qualify for and claim the Alaska Veteran Preference, you must answer **YES** to the below questions as well as answer **YES** to all the questions in the Alaska Veteran Preference section above.

**Per AS36.30.321(F), is your business:**

1	A sole proprietorship owned by an Alaska veteran?	<input type="checkbox"/> Yes <input type="checkbox"/> No
2	A partnership under AS32.06 or AS32.11 and a majority of the members are Alaska veterans?	<input type="checkbox"/> Yes <input type="checkbox"/> No
3	A limited liability company organized under AS10.50 and a majority of the members are Alaska veterans?	<input type="checkbox"/> Yes <input type="checkbox"/> No
4	A corporation that is wholly owned by individuals, and a majority of the individuals are Alaska veterans?	<input type="checkbox"/> Yes <input type="checkbox"/> No

**Per AS36.30.321(F)(3), an “Alaska veteran” is defined as an individual who:**

- A. Served in the:
  - a. Armed forces of the United States, including a reserve unit of the United States armed forces ; or
  - b. Alaska Territorial Guard, The Alaska Army National Guard, the Alaska Air Nations Guards, or the Alaska Naval Militia; and,
- B. Was separated from services under a condition that was not dishonorable.

4	Do you certify the individual(s) indicated in items 1-4 above meet this definition and can provide documentation of their service and discharge in necessary?	<input type="checkbox"/> Yes <input type="checkbox"/> No
---	---	--

**Alaska Military Skills Program Preference Questions**

To qualify for and claim the Alaska Military Skills Program Preference, you must answer **YES** to the below questions as well as answer **YES** to all the questions in the Alaska Bidder Preference section above.

**Per 36.30.321(I), does your business:**

1	Employ at least one person who is enrolled in, or within the past two years, graduated from, a United States Department of Defense SkillBridge or United States Army career skills program that offers civilian work experience through specific industry training, pre-apprenticeships, registered apprenticeships, or internships during the last 180 days before a service member separates or retires from the service; or	<input type="checkbox"/> Yes <input type="checkbox"/> No
2	Have an active partnership with an entity that employs an apprentice through a program described in item 1 above?	<input type="checkbox"/> Yes <input type="checkbox"/> No
3	Have proof of an employee’s graduation or enrollment in a qualified program as described in 1. above?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Do not edit the bid in any manner. In accordance with 2 AAC 12.830 alternate bids (bids that offer something different than what is asked for) will be rejected. Contact the Procurement Specialist in writing with any questions.

<b>BID SCHEDULE</b>
---------------------

Item #	Estimated TOTAL Quantity	Description	UNIT Price
1)	200,000	<b>Printing of Pages</b>	\$_____ /ea
	\$_____		
2)	70,000	<b>Folding and Inserting Notices</b>	\$_____ /ea
	\$_____		
3)	70,000	<b>Envelopes (#10 window)</b>	\$_____ /ea
	\$_____		
4)	70,000	<b>Postage</b>	\$_____ /ea
	\$_____		
			TOTAL COST: \$_____



**AK | DFCS**  
ALASKA DEPARTMENT OF  
FAMILY AND COMMUNITY  
SERVICES

**Reference A**  
**Information Technology Requirements**  
State of Alaska  
Department of Family and Community Services

**TABLE OF CONTENTS**

1	Purpose of IT Requirements .....	2
1.1	IT Requirements Intent and Approach.....	2
2	Technical Qualifications Response.....	4
2.1	Minimum Qualifications.....	4
2.2	Understanding of the Technical Aspects of the Project.....	4
3	State of Alaska DFCS Technology Services, Standards, and IT Road Map.....	5
3.1	DFCS Information Technology Services Staffing Support.....	5
3.2	Engagement and Service Delivery Management Services and Standards .....	6
3.3	Project Portfolio Management Services and Standards .....	7
3.4	Asset Management Services and Standards .....	8
3.5	Systems Integration and DDI Services and Standards.....	10
3.6	Systems Operations and Administration Services and Standards.....	14
3.7	Information Security Compliance and Privacy Services and Standards .....	16
3.8	Enterprise Desktop and Mobility Services and Standards .....	20
3.9	DFCS Hosting and Datacenter Services and Standards .....	22
3.10	DFCS Wide Area Network, Telecommunications, and Perimeter Security Services and Standards .....	23
3.11	Accessibility.....	24
3.12	State of Alaska DFCS MITA Standards and Department IT Technology Standards.....	25

## 1 Purpose of IT Requirements

The State of Alaska Department of Family and Community Services (DFCS) is engaged in a Cloud First initiative strongly favoring SaaS solutions. We have embraced an Information Technology (IT) Roadmap for shared services using our Enterprise Service Bus (ESB), and Master Client Index (MCI).

The response to this request must address if, and how, the proposed product solution will integrate into this environment, where appropriate.

### 1.1 IT Requirements Intent and Approach

DFCS Information Technology Services (ITS) values our partner relationships with external vendors, contractors, and grantees. DFCS ITS is focused on providing the best value to our customers by supporting IT procurements from the RFP solicitation process, through project initiation, planning, execution, and closing.

At a high-level, these IT requirements support the proposal solicitation by meeting two goals:

1. The requirements help the Offeror understand our service delivery approach. They give Offerors the opportunity to shape their proposals to best fit the team of program staff, ITS staff, and Offeror staff that will work together to deliver the solution.
2. The requirements identify specific requirements and statements that Offerors must address to be classified as responsive.

These IT requirements are structured into services and standards sections, corresponding to a service line within DFCS ITS. For example, the solicitation-relevant requirements for end-user desktop configurations are in the “Enterprise Desktop Services and Standards” section.

As part of our Cloud First initiative, DFCS IT is seeking proposals for solutions which are vendor hosted and vendor managed, rather than provided locally or hosted within the department’s network.

However, we recognize that solutions are available in many forms. Offerors may consider proposing one or more of the following options:

- DFCS hosted and managed solution components;
- 3<sup>rd</sup> party hosted, DFCS managed solution components;
- Software as a Service (SaaS)
- Anything as a Service (XaaS);
- Hybrid/Combination of above.

DFCS recognizes that SaaS and XaaS delivery models afford some additional value to our department. It offers the opportunity to leverage the business value of the solutions without bearing the costs and risks of having to maintain development and operational infrastructure. This value is achieved when the SaaS/XaaS vendor carries the burden of managing technical operations and ongoing development/maintenance, while collaborating with their clients to meet and maintain the functional requirements and integrity of the solution.

Offerors should read each section carefully to understand how DFCS ITS applies a particular service-line to procured services and what specific requirements, questions, and statements must be answered. Please be aware that the State of Alaska requires all resources utilized as a part of the RFP response, system development, and implementation to be US based or DFCS approved resources. This includes

hosted services, vendor personnel, vendor contracted services, and personnel and vendor contracted consulting services.

## **2 Technical Qualifications Response**

### **2.1 Minimum Qualifications**

Offerors must complete **Required Vendor Response - DFCS IT Requirements**, which correspond to the requirements described in Section 3 of this document and return it as part of their proposal. A failure to complete and return this IT Reference will result in a proposal being deemed non-responsive.

### **2.2 Understanding of the Technical Aspects of the Project**

In the body of their proposal, Offerors must provide comprehensive narrative statements that illustrate their understanding of the technical requirements and must respond to all applicable sections, or respond why a section is not applicable.

A failure to demonstrate how the solution being proposed addresses the Technical Requirements outlined may result in the proposal deemed non-responsive and rejected.

### 3 State of Alaska DFCS Technology Services, Standards, and IT Road Map

Information technology services for DFCS agencies are provided by DFCS Division of Finance and Management Services Information Technology Services (ITS). DFCS ITS provides the following functions: maintenance of the DFCS Data Centers in Juneau and Anchorage; project execution support; operational support; and integration assistance for systems hosted on site. We also manage some IT services hosted and operated out of the State of Alaska Office of Information Technology (SOA-OIT) data centers (separate from our datacenters), and services out of Microsoft's Azure Government Community Cloud.

This section describes many of the services offered in detail and highlights elements of our IT Environment we think you need to know to work with us.

#### 3.1 DFCS Information Technology Services Staffing Support

Regardless of whether the Offeror proposes a totally outsourced, partially outsourced, or hosted on DFCS Premise solution, expectations for support must be clearly defined.

DFCS ITS staffing support hours are:

- Customer & Application Support hours are M-F, 8:00am to 5:00PM Alaska Time
- Network Support hours are M-F, 7:00AM to 5:00PM Alaska Time

Support from DFCS ITS required outside of those hours, including evening and weekend batch job support, must be defined and documented. This must include the duties and expectations for DFCS ITS staff. All hours of operation **must be expressed in Alaska Time**.

##### ***3.1.1 Requirement – Production Operations Phases***

The Offeror must:

- Define and document a schedule of hours they plan to operate, including the time zone(s) they plan to operate from;
- Identify hours their staff will work outside of the DFCS ITS standard hours, defined in this section;
- Identify the daily schedule of hours during which they expect DFCS ITS and DFCS Program staff to support the activities under the execution of the proposal;
  - The schedule will include and differentiate hours for end-user access and hours for technical support, including any offline batch or after-hours system maintenance activities.
- Commit to deliver a plan that includes Offeror and DFCS agreed upon daily scheduled hours.
  - The plan must also include the schedule of Offeror and State of Alaska observed holidays.
  - SOA Holidays can be found at: <https://doa.alaska.gov/calendar/>
- ***If solution is to be DFCS managed in the Production and Operations phase***, additional requirements are:
  - The Offeror's proposal must include a solution that requires no regular after-hours system support
  - If the Offeror's proposed solution requires after-hours system support, the Offeror must reach formal agreement via:
    - An accepted Operations Support Model deliverable;
    - The OIT Department Technology Officer for DFCS and DFCS Assistant Commissioner approval.
    - This agreement must be reached at least 6 months prior to commencement of proposed training activities that precede DFCS assuming operational responsibilities for the solution.

### **3.2 Engagement and Service Delivery Management Services and Standards**

Engagement and Service Delivery Management Services includes the activities DFCS ITS performs to engage with our DFCS Program staff and manage delivery of all IT services. This includes defining the organization's requirements, assisting with DFCS IT Governance alignment, change request processes, and applying and managing the correct DFCS ITS service-lines for specific DFCS ITS initiatives and procurements.

#### **3.2.1 Contract Negotiations ITS Review and Approval**

DFCS ITS participates directly on the contract negotiations team to review and approve all IT related contract elements further specified in the final contract.

##### **3.2.1.1 Requirement – IT Contract Review**

The Offeror must be prepared to work with DFCS ITS, Procurement, and Program staff to review and approve all IT related contract elements.

#### **3.2.2 Project Kickoff Service Alignment Conference**

As part of project kickoff activities, DFCS ITS and Program representatives will meet with the Offeror's execution team to agree upon the necessary DFCS ITS service lines required to support the execution of the procurement. This activity will be based on a review of the scope and schedule defined in the solicitation, the proposal, and the final contract.

The outcome will be a list of DFCS ITS service lines supporting execution of the procurement and a list of any gaps identified by the Service Alignment Conference team. Gaps identified may include services or products DFCS ITS does not support, DFCS ITS staffing resource constraints, or other gaps.

##### **3.2.2.1 Requirement – DFCS ITS Service Alignment Conference**

The Offeror must include project activities to reach agreement with DFCS ITS and DFCS Program staff on DFCS ITS support service lines and identify any gaps. All gaps identified must include a plan of action to address and resolve the gaps.

#### **3.2.3 DFCS Service Line Engagement and Planning**

Different procurements require customized support activities to succeed within scope, schedule, and resource constraints. To ensure the best outcome, the DFCS ITS service lines identified to support the procurement will work with DFCS Program staff and Offeror staff to roadmap the service line engagement schedule, review the gaps identified in the service alignment conference, and detail the action plans to address those gaps.

##### **3.2.3.1 Requirement – DFCS IT Service Line Engagement and Planning Workshops**

The Offeror must include project activities to reach agreement with DFCS ITS and Program staff on the service line engagements identified in the Service Alignment Conference deliverables. These activities must roadmap the schedule of service line engagements, identify the service line team members, review the gaps previously identified, and detail the action plans to address those gaps.

#### **3.2.4 DFCS Service Line Management Processes and Tools**

DFCS ITS service line staff will use their standard, defined processes and management tools to document and manage their work (See Sections 2.1 and 2.2 of Information Technology Standards Reference D).



For cost and operational efficiency, DFCS ITS prefers that the Offeror align their processes and tools with those of DFCS ITS. The Offeror may propose leveraging the DFCS processes and tools in their proposal.

**3.2.4.1 Requirement – Service Line Management Processes and Tools Alignment**

DFCS prefers the Offeror be prepared to work with DFCS ITS service line management processes and tools. For each DFCS IT service line supporting the project, the Offeror must review the applicable processes and tools with DFCS ITS and DFCS Program staff to align processes and tools of the project with those used by DFCS ITS.

If the Offeror and DFCS Program staff determine a benefit to using alternate tools, the Offeror must accept the cost of any duplication of effort required of either the Offeror's staff or DFCS Program staff to maintain and synchronize requirements, documentation, service requests or other artifacts applicable to the DFCS ITS service line.

Whichever tools are selected, the Offeror must document agreed upon decisions made with DFCS ITS and DFCS Program staff.

**3.2.5 DFCS Managed Off-site Hosting Scenarios**

All DFCS Engagement and Service Delivery Management Services and Standards apply to DFCS managed off-site hosting scenarios.

**3.2.5.1 Requirement**

The Offeror must understand and acknowledge 3.2.5.

The Offeror must identify any elements of your proposed solution that will be hosted outside of DFCS datacenters.

The Offeror must identify the geographic location of each of those elements.

**3.2.6 Software as a Service (SaaS) and Anything as Service (XaaS) Scenarios**

All DFCS Engagement and Service Delivery Management Services and Standards apply to SaaS/XaaS scenarios.

**3.2.6.1 Requirement**

The Offeror must understand and acknowledge that all DFCS Engagement and Service Delivery Management Services and Standards apply to SaaS and XaaS scenarios.

Identify any elements of your proposed solution that will be fulfilled via Software-as-a-Service delivery models.

**3.3 Project Portfolio Management Services and Standards**

See IT Reference B—DFCS Project Management Requirements.

**3.3.1 DFCS Managed Off-site Hosting Scenarios**

All DFCS Project Portfolio Management Services and Standards apply to DFCS managed off-site hosting scenarios.

**3.3.1.1 Requirement**

The Offeror must understand and acknowledge 3.3.1.

**3.3.2 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios**

All DFCS Project Portfolio Management Services and Standards apply to SaaS/XaaS scenarios.

**3.3.2.1 Requirement**

The Offeror must understand and acknowledge 3.3.2.

**3.4 Asset Management Services and Standards**

Asset Management Services include the activities DFCS ITS performs to manage software licensing and other software and information assets. DFCS considers all data, software source code, configuration files, binaries, licenses, and configured systems as “assets”. DFCS Policies and Standard Operating Procedures require that stewards, responsible for creating and maintaining assets, properly manage these assets. This means asset stewards should apply proper inventory and version control practices to ensure individual assets are identified and version consistent artifact sets can be recreated to support disaster recovery, testing, audit, and other scenarios.

**3.4.1 Artifact Version Management**

DFCS ITS operates a document and code management repository that supports version control (see Information Technology Standards Reference D). The Offeror must transfer ownership of all project artifacts to DFCS as part of the scope of work, including the effort to convert/migrate the artifacts into the DFCS artifact version management repository. To reduce project overhead and transition costs, the Offeror is encouraged to use the DFCS artifact version management repository during project execution.

**3.4.1.1 Requirement**

Requirements, design documents, source code, configuration files, and binaries that are versioned over time must be managed in one or more version control repositories such that any released version of these artifacts can be retrieved later to rebuild the information system or application. Platforms that support configuration changes via a graphical user interface must support an extract of the changes made that can be loaded into the version control repository and release-managed in an equivalent manner to source code.

**3.4.2 Licensing Agreement**

**3.4.2.1 Requirement**

The license shall include, but not be limited to:

- All supporting programs in the most current version;
- All scripts, programs, transaction management or database synchronization software, and other system instructions for operating the system in the most current version;
- All data files in the most current version;
- User and operational manuals and other documentation;
- System and program documentation describing the most current version of the system,
- The most current versions of source and object code;
- Training programs for the State and other designated State staff, their agents, or designated representatives, in the operation and maintenance of the system;
- All performance-enhancing operational plans and products, exclusive of equipment; and
- All specialized or specially modified operating system software and specially developed programs, including utilities, software, and documentation used in the operation of the system.

Ongoing upgrades of the application software and supporting 3<sup>rd</sup> party programs must be provided through the end of the contract.

Any other specialized software to be integrated into the system, and not covered under a public domain license, must be identified as to its commercial source and the cost must be identified in the Cost proposal. DFCS may, at its option, purchase commercially available software components itself.

The contractor must convey to DFCS, upon request and without limitation, copies of all interim work products, system documentation, operating instructions, procedures, data processing source code, and executable programs that are part of the system, whether they are developed by the employees of the contractor or any subcontractor as part of this contract or transferred from another public domain system or contract. The provision of this section related to ownership/support for the product must be incorporated into any subcontract that relates to the development, operation, or maintenance of any component part of the system.

### **3.4.3 Software Procurement Assurance – Guaranteed Access to Software**

#### ***3.4.3.1 Requirement***

DFCS shall have full and complete access to all source code, documentation, utilities, software tools, and other similar items used to develop/install the proposed solution or may be useful in maintaining or enhancing the equipment and solution after it is operating in a production environment.

DFCS executive leadership may choose to waive the above requirement upon written request explaining your unique business need. SaaS/XaaS solutions may also request waivers for these requirements (see 3.4.7).

In such cases any of the above-mentioned items not turned over to DFCS upon completion of the installation, the Offeror must provide a written guarantee to DFCS of uninterrupted future access to, and license to use, those items. The guarantee must be binding on all agents, successors, and assignees of the contractor and subcontractor. State access to source code may be protected by use of a third-party escrow account.

If an escrow account is used, the terms must include at a minimum:

- Update of the source code in escrow as often as required for the source code to reflect the current version of each application of the software licensed by DFCS.
- DFCS has the right to view or access the source code to:
  - Verify the source code's completeness and readability of the media.
  - Obtain a copy of the source code in the event of a filing of Bankruptcy where the Offeror is no longer able to provide acceptable service.
  - Obtain a copy of the source code if the Offeror ceases to do business completely, or to do business in the line of business marketplace the system supports.

DFCS reserves the right to consult legal counsel as to the sufficiency of the licensing agreement and guarantee of access put forth by the Offeror.

### **3.4.4 Software Procurement Assurance – Federal Rights**

#### ***3.4.4.1 Requirement***

If a federal grant was used for this solution, the federal government reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, or otherwise use, and to authorize others to use, for federal government purposes, the copyright in any work developed under a grant, sub-grant.

### **3.4.5 Data Ownership**

#### ***3.4.5.1 Requirement – Data Ownership***

DFCS shall have unlimited rights to use, disclose or duplicate, for any purpose whatsoever, all information and data developed, derived, documented, installed, improved, or furnished by the Offeror under this contract. All files containing any DFCS information are the sole and exclusive property of DFCS. The Offeror agrees not to use information obtained for any purposes not directly related to this contract without prior written permission from DFCS. Offeror agrees to abide by all federal and state confidentiality requirements. In addition, the Offeror agrees to provide to DFCS, at the end or at any time during the contractual period, the data managed by the solution, in whole or in part, in a format agreed upon by both parties.

### **3.4.6 DFCS Managed Off-site Hosting Scenarios**

All DFCS Asset Management Services and Standards apply to DFCS managed off-site hosting scenarios.

#### **3.4.6.1 Requirement**

The Offeror must understand and acknowledge 3.4.6.

### **3.4.7 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios**

DFCS ITS expects that by owning ongoing maintenance and technical operations, SaaS/XaaS solutions implicitly provide a limited degree of freedom to deviate from DFCS ITS Asset Management Services and Standards.

#### **3.4.7.1 Requirement**

If proposing SaaS/XaaS components for all or part of the solution, the Offeror's proposal must comply with all Asset Management Services and Standards requirements.

The Offeror may propose leveraging variations or exceptions under this subsection, *Software as a Service Scenarios (SaaS) and Anything as a Service (XaaS)*. If the Offeror wishes to leverage variations or exceptions, these must be defined. If exceptions are to be requested please clearly outline

- Which requirement you are seeking an exception for
- What alternative measure you are offering in its place
- How the department's interests will be protected, even in the event the Offeror goes out of business or files for bankruptcy

#### **3.4.7.2 Requirement – Data Stewardship**

The Offeror will maintain Alaska's data in the solution for the life of the contract. The Offeror must explain how data will be archived for the solution. Turnover requirements will be negotiated between DFCS and the Offeror to ensure that all DFCS data will be returned to DFCS in a cooperative manner at the close of the contract or the decommissioning of the solution. DFCS data may include; deliverables, reports, configuration details, business requirement documents, test plans, scripts, and results.

#### **3.4.7.3 Requirement – Geographic Location Identification**

The Offeror must identify the geographic location of any non-DFCS hosted external information systems that receive, process, store, or transmit proposed solution data.

## **3.5 Systems Integration and DDI Services and Standards**

DFCS ITS provides a full range of Systems Integration and Design, Development, and Implementation (DDI) Services. These services follow DFCS standards to ensure maximum leverage of staff and other resources and ensure scalability. DFCS expects the Offeror to understand and align their proposal and activities with DFCS Systems Integration and DDI Services and standards.

The most noted points of integrations include:

- Our department's information exchange architecture;
- Master data management;
- Integrated Resource Information System (IRIS) and Alaska Data Enterprise Reporting (ALDER) integration;
- Authentication and Single Sign-On.

Maintaining alignment will be an ongoing activity during the project. However, the Offeror must demonstrate how they anticipate reaching alignment within their proposal.

### **3.5.1 Information Exchange Architecture**

To simplify the effort and reduce costs of DFCS systems implementation and long-term operations, DFCS has implemented an Enterprise Service Bus (ESB) that supports system integration and information exchange. Additionally, DFCS has partnered to create an Alaska statewide Health Information Exchange (HIE). Together, the ESB and the HIE can substantially reduce the operational complexity of moving data between systems hosted on-premise or in the cloud.

#### **3.5.1.1 Requirement**

Data exchange interfaces must leverage the DFCS Enterprise Service Bus and/or the statewide HIE, where applicable.

The Offeror must describe

- What interfaces and data exchange processes do you anticipate implementing with the HIE?
  - If you do anticipate implementing these processes, please describe how the proposed solution would transfer data to and from the HIE, as applicable.
- What interfaces, data exchange processes and services do you anticipate implementing via the DFCS Enterprise Service Bus (ESB)?
  - If you do anticipate implementing these processes, please describe how the solution would transfer data using this method?
- Your architectural approach to transferring data sets to/from your system. Include both single-record/case and batch transfer scenarios.

### **3.5.2 Master Data Management**

DFCS has implemented master data management services for client/consumer/person demographic records via the DFCS Master Client Index (MCI). The MCI connects client demographic records across applications and systems.

Solutions that create, read, or update client, consumer, or other person demographic data must integrate with the MCI to ensure their demographic records are registered in the MCI and appropriately merged with matching client records in the index.

Such solutions must integrate with the DFCS MCI and ensure the end-users of the solution can leverage the Person service operations to register and maintain their person demographic records in the MCI. This must include interactions that update the MCI when record duplication, deactivation, and similar record management scenarios occur within the scope of the Offeror's proposed solution.

#### **3.5.2.1 Requirement – Master Client Index (MCI) Integration**

The Offeror must integrate their proposed solution with the DFCS Master Client Index (MCI) if the Offeror's proposed solution will store person demographic data of clients, members, beneficiaries, or other individuals who:

- Apply for or receive DFCS program services or benefits; or
- Are the subject of a DFCS registry; or
- Are a participant in a case, filing-unit, or other group for which DFCS expends funds or must measure services.

The Offeror must:

- Indicate whether your proposed solution will include demographic records for individuals.
- Indicate whether your proposed solution will integrate with the DFCS Master Client Index.
  - If your solution will not integrate with the DFCS MCI, please indicate why.
  - If your solution will integrate with the DFCS MCI, please describe your process to register and merge client demographic information records with the MCI.
    - Include the technical approach and the high-level search, create, update, and synchronization procedures for managing MCI relevant demographic data in your solution.

### **3.5.3 IRIS and ALDER Integration**

DFCS uses the State of Alaska Enterprise Resource Planning (ERP) system, IRIS, for managing finance, accounting, property-asset, and HR management functions. DFCS uses the State of Alaska ALDER data warehouse for reporting and extracting finance, accounting and HR data.

Solutions that include these functions should plan for a gap analysis to determine the appropriate integration approach that avoids duplication of services and addresses developing and integrating complementary solution services and functions.

#### **3.5.3.1 Requirement**

Offerors whose proposed solution includes finance, accounting, and HR functions must plan to conduct a gap analysis activity with DFCS ITS, DFCS Program staff, and Department of Administration Division of Finance IRIS support subject matter experts. This analysis is to determine which system will own which processes, how the systems will integrate and where the data will live.

Offeror's proposal must include activities to support this gap analysis and associated DDI activities to interface between IRIS, ALDER and the proposed solution.

### **3.5.4 Authentication and Single Sign On**

DFCS has established a standard authentication platform, using Microsoft's Active Directory (AD) to support authentication for DFCS hosted systems.

DFCS has established a standard federated authentication platform, Microsoft Active Directory Federation Services (ADFS), to support single sign on authentication scenarios for DFCS employees who use systems external to the department that cannot integrate with the DFCS Active Directory.

Integration with either of these methods provides a uniform authentication mechanism for DFCS staff and sponsored external partner/contractor staff to manage authorized access to department information systems. Leveraging the DFCS AD allows the Offeror's solution to inherit the account management, authentication, and audit-logging features of the DFCS AD to validate authorized access and meet several technical security controls.

#### **3.5.4.1 Requirement – Single Sign-On and Authentication**

The Offeror must integrate their solution with the Alaska DFCS Active Directory or DFCS Active Directory Federated Services (ADFS). The integration must support authentication access requests prior to authorization.

The Offeror will include cost and activities in their proposal to support the DFCS AD integration.

### **3.5.5 Technical Services and Development Platform**

DFCS expects the Offeror to align their proposal with this DFCS standard technical services platform to the maximum extent possible.

DFCS ITS operates a leading software development lifecycle (SDLC) management platform. See IT Reference D for details on this tool. To reduce project overhead and transition costs, the Offeror is encouraged to consider using the DFCS artifact version management repository.

#### ***3.5.5.1 Requirement – Development Platform***

The Offeror will use the software identified in IT Reference D for the development and deployment of this application. The Offeror must state which version the application components are designed in and how this solution will be accessed in the DFCS environment. You will need to identify what skills and expertise would be needed to support your proposed infrastructure.

For each non-DFCS standard software component in the proposed solution:

- Describe the purpose of the non-standard component;
- Propose a component in the DFCS IT standards that could be used instead of the non-standard component;
- Include an optional cost adjustment to implement the solution using that DFCS standard component within the cost proposal section of the RFP;
- If there is no DFCS standard software component identified that meets the function of the non-standard component proposed, identify a Microsoft component that meets the purpose of the non-standard proposed component;
- Include an optional cost adjustment to implement the solution using that Microsoft component within the cost proposal section of the RFP; and
- If no Microsoft component exists that meets the purpose of the proposed non-standard component, indicate there is no equivalent component available.

#### ***3.5.5.2 Requirement – Software Development Lifecycle (SDLC)***

The Offeror must apply a methodology that demonstrates key elements of the SDLC, including:

- Gathered and validated requirements and acceptance criteria artifacts;
- Documented and validated design artifacts;
- Documented development and build tools and processes;
- Versioned and managed development artifact change sets;
- Documented deployment and promotion processes for moving builds and release candidates from lower environments to higher-confidence environments and ultimately production (e.g., development > system integration test > user acceptance test > production & training);
- Documented quality assurance, system test, and user acceptance test script and results artifacts;
- Documented release management procedures.

The Offeror must use a set of industry standard tools to track and manage artifacts of the SDLC and must align this toolset with the standard DFCS SDLC tools.

#### ***3.5.5.3 Requirement – Secure Systems Development Lifecycle***

The Offeror must complete software development in compliance with DFCS Secure Systems Development Lifecycle, including:

- **Secure Coding** - The Offeror shall disclose what tools are used in the software development environment to encourage secure coding.
- **Disclosure** - The Offeror shall document in writing to the Purchaser all third-party software used in the software, including all libraries, frameworks, components, and other products, whether commercial, free, open-source, or proprietary.
- **Evaluation** - The Offeror shall make reasonable efforts to ensure third party software meets all the terms of this agreement and is as secure as the custom code developed under this agreement.
- **Source Code Scanning** - The Offeror shall work with DFCS staff to facilitate static code scanning for all product and 3<sup>rd</sup> party files using a DFCS provided scanning solution.
- **Hosting Environment Hardening** – The Offeror shall work with DFCS staff to ensure that any hosting environment utilized complies with department adopted standards for security hardening.
- **Vulnerability and Penetration Testing** – for SaaS and XaaS environments, the Offeror shall facilitate requests for 3<sup>rd</sup> party vulnerability and/or penetration testing of DFCS solutions.

### **3.5.6 DFCS Managed Off-site Hosting Scenarios**

All DFCS Systems Integration and DDI Services and Standards apply to DFCS managed off-site hosting scenarios.

#### **3.5.6.1 Requirement**

The Offeror must understand and acknowledge 3.5.6.

### **3.5.7 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios**

DFCS IT expects that, by owning ongoing maintenance and technical operations, SaaS solutions implicitly provide a limited degree of freedom to deviate from DFCS IT Systems Integration and DDI Services and Standards. Specifically, when federal funding rights do not apply, and when DFCS is not performing technical services administration within the SaaS hosting environment, SaaS solutions may employ non-compliant infrastructure and non-compliant platform components in their design and implementation.

#### **3.5.7.1 Requirement**

When federal funding rights apply, see *section 3.4.4 Software Procurement Assurance – Federal Rights*, the Offeror’s proposed solution must employ DFCS IT Systems Integration and DDI Services and Standards compliant platform components. This requirement supports State of Alaska maintenance risk mitigation in the event the Offeror determines to discontinue the service at a future date, and DFCS must assume maintenance and/or operations. If the Offeror cannot meet this requirement, they may propose an operational contingency statement the State of Alaska can consider as a viable risk mitigation alternative to assuming the future maintenance risks.

## **3.6 Systems Operations and Administration Services and Standards**

System Operations and Administration Services includes the activities DFCS ITS performs to support technical system operations and system administration. This section describes information system administration services that support solutions operating in production.

### **3.6.1 Administration Services and Standards**

DFCS ITS operates and manages technical services for DFCS information systems and applications. This includes ongoing administration, configuration monitoring and security patching of the underlying software components of the solution.



See IT Reference D for the list of technical service components administered by DFCS IT within the System Operations and Administration Services service line.

**3.6.1.1 Requirement – Centralized Technical Administration**

The Offeror must understand that information technology administration duties are restricted to qualified individuals within the centralized DFCS ITS section. DFCS Program staff outside the DFCS ITS section are not authorized to manage or administer technical information technology services. Examples of technical services include, but are not limited to administration of: relational database management systems (Oracle, SQL Server, MySQL, PostgreSQL, etc.); application servers (ASP.NET, JEE, PHP, etc.), and desktop and server operating systems.

Non-ITS, DFCS Program staff may be delegated administration of business services via secured, audited user-interfaces in the application, such as interfaces to create user accounts within the application, assign security roles within the application, maintain code-lookup tables, and other business administration functions. All business administration changes must be completed via a privileged, secured application user-interface that logs all data changes and which user made the change.

The Offeror must validate all technical administration designs with DFCS IT stakeholders in the System Operations and Administration Services service line.

The Offeror must include appropriate documentation and training for DFCS ITS staff in the technical services administration for the proposed solution.

**3.6.1.2 Requirement – Authorized Access**

The Offeror must follow DFCS standard operating procedures for obtaining and terminating access to DFCS facilities and systems. To support proper access management, the Offeror must notify the DFCS contract administrator of any personnel transfers or termination of Offeror personnel, including sub-contractors, who possess DFCS credentials and/or badges, or who have DFCS information system privileges, within fifteen (15) calendar days. Notification must be in writing. This personnel transfer and termination notification requirement may not be extended and does not supersede other Offeror personnel notification requirements with stricter timelines within the contract. (NIST 800-53 r4 PS 07 D)

**3.6.2 DFCS Managed Off-site Hosting Scenarios**

All DFCS Systems Operations and Administration Services and Standards apply to DFCS managed off-site hosting scenarios.

**3.6.2.1 Requirement**

The Offeror must understand and acknowledge 3.6.2.

**3.6.3 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios**

DFCS ITS expects that, by owning ongoing maintenance and technical operations, SaaS/XaaS solutions implicitly provide a limited degree of freedom to deviate from DFCS ITS Systems Operations and Administration Services and Standards. Specifically, when federal funding rights do not apply, and when DFCS is not performing technical services administration within the SaaS/XaaS hosting environment, SaaS/XaaS solutions may employ non-compliant infrastructure and non-compliant platform components in their design and implementation.

**3.6.3.1 Requirement**

When federal funding rights apply, *see section 3.4.4*, the Offeror’s proposed solution must employ DFCS ITS Systems Integration and DDI Services and Standards compliant platform components. This requirement supports State of Alaska operational risk mitigation in the event the Offeror determines to discontinue the service at a future date, and DFCS must assume maintenance and/or operations. If the Offeror cannot meet this requirement, they may propose an operational contingency statement the State of Alaska can consider as a viable risk mitigation alternative to assuming the future operational risks.

### **3.7 Information Security Compliance and Privacy Services and Standards**

Information Security Compliance and Privacy Services include the activities DFCS ITS performs to support legal compliance with information security, privacy, and ongoing development/maintenance of security policy and practice. DFCS maintains a robust information security compliance and privacy program. This section describes the information security compliance and privacy services and standards applied throughout the lifecycle of each DFCS information system.

#### **3.7.1 Data Retention/Destruction**

Destruction of Electronic Protected Health Information (ePHI) and Personally Identifiable Information (PII) on electronic media requires that the organization employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

##### **3.7.1.1 Disposing of Printed Information**

All protected printed media (ePHI, PII, PI, PCI, CJI, etc.) must be disposed of in a manner consistent with the guidance provided by the NIST Special Publication 800-88 Revision 1 (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>).

##### **3.7.1.2 Disposing of Information on Electronic Media**

All protected electronic media (ePHI, PII, PI, PCI, CJI, etc.) must be disposed of in a manner consistent with the guidance provided by the Department of the Army’s brief, Cybersecurity: Sanitization of Media ([https://armypubs.army.mil/epubs/DR\\_pubs/DR\\_a/pdf/web/ARN6681\\_Pam25-2-8\\_WEB\\_FINAL.pdf#:~:text=The%20procedures%20in%20this%20chapter%20establish%20the%20requirement,the%20disposal%20and%20handling%20of%20hazardous%20IT%20waste](https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN6681_Pam25-2-8_WEB_FINAL.pdf#:~:text=The%20procedures%20in%20this%20chapter%20establish%20the%20requirement,the%20disposal%20and%20handling%20of%20hazardous%20IT%20waste)) and NIST Special Publication 800-88 Revision 1 (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>). Disposed of electronic media must receive a Certificate of Media Disposal or agreed upon proof of disposal for each device disposed.

##### **3.7.1.3 Requirement – Record Retention**

The Offeror must comply with the DFCS policies and procedures for record retention and disposal of sensitive information (IT Reference F—Data Destruction Information and References), if applicable.

##### **3.7.1.4 Requirement – Data Destruction**

The Offeror must provide procedures and agree to all data (including test data) destruction when contract ends if continuing operations and maintenance is not provided by the contractor.

#### **3.7.2 Security Controls**

Department, State, and Federal security standards are enforced through State of Alaska and DFCS policy and procedure. The procedures leverage FIPS 199 information security categorization and NIST 800-53 information security controls documentation. The DFCS Governance, Risk, and Compliance system serves as the system of record to capture this documentation in an “authorization package”.

##### **3.7.2.1 Requirement – Authorization Package**

Within the proposed scope of work and activities, the Offeror must:

- Work with the Department Security Office (DSO) to document the approach, methodology, roles, responsibilities, processes, and tasks the Offeror will assume to complete the authorization package;
- Develop and submit a complete Authorization Package for review and approval by the DSO;
- Submit to the DFCS Security Designee, a thoroughly completed Authorization Package for review and comment within four (4) weeks of the project's initiation and receipt of the Authorization Package questionnaire.
  - Offeror shall respond to clarification questions within two (2) weeks of receipt of DFCS comments on the Authorization Package.

Security controls are reviewed for risk regardless of whether an application/solution is hosted on premise or elsewhere. A paper version of the Authorization Package is included in IT Reference H – DFCS Sample Security Authorization Package.

**3.7.2.2 Requirement – Code Vulnerability Scanning**

DFCS employs a code vulnerability scanning engine. The Offeror shall process all scannable code through the DFCS static code vulnerability scanning engine. Findings from the code vulnerability scan will be attached to the systems Authorization Package for review and acceptance from the DFCS Department Security Office (DSO).

**3.7.2.3 Requirement – Security Control Verification**

After the Authorization Package is complete, it is subject to review and acceptance from the DFCS Department Security Office (DSO). Approval to operate in the DFCS environment is predicated on acceptance of the Authorization Package responses as well as compliance with the processes outlined in *section 3.5.5.3* of this document. These processes may require changes and updates to the system by the Offeror in order to comply with regulatory requirements.

The Offeror must plan activities to work towards security compliance requirements and accommodate an appropriate number of remediation cycles to address any identified defects.

Please note, although workload varies in proportion to the size of the solution, we have found that most small to medium size solutions require 80 to 120 hours to complete the initial security control responses.

**3.7.2.4 Requirement – Business Associate Agreement**

If data is determined to be ePHI, the DFCS Business Associate Agreement must be signed at contract. Other types of data must be treated with appropriate confidential data handling and may be covered by a data usage agreement.

**3.7.2.5 Requirement – Authority to Operate**

Once all security compliance is established via an approved Authorization Package and signed Business Associate Agreements (BAA) or data usage agreements (as applicable), the solution will be granted an Authority to Operate (ATO) by the DFCS designated Division Data Owner, the Department Chief Information Security Officer, and the OIT Department Technology Officer for DFCS. The Offeror must plan activities and milestones that support obtaining the ATO prior to production rollout.

The Offeror must plan for delays associated with a solution's inability to initially obtain ATO. These delays must take into consideration the business's implementation targets. It is imperative that authorization package responses be scheduled with ample time for completion, DSO review, and mitigation to not negatively affect the business's implementation targets.

### **3.7.3 Auditing and Logging Integration**

For logging and audit, DFCS uses an industry standard Security Information and Event Management (SEIM) system. All systems are required to be capable of logging and auditing in a concise summary that can be easily integrated into the DFCS SEIM. The package produced by the application must be inclusive of all the data for who is accessing, reading, and writing data.

#### **3.7.3.1 Requirement**

The Offeror's proposed solution must integrate with DFCS's SEIM infrastructure. The Offeror's proposed solution must include activities to collaborate with DFCS ITS in establishing log collection activities for standard log formats and customizing log parsing for non-standard log formats.

### **3.7.4 Data Security**

Sensitive and/or confidential data includes (but is not limited to) Electronic Protected Health Information (ePHI) as defined in the Federal Health Insurance Portability and Accountability Act (HIPAA), Personally Identifiable Information (PII) as defined by the US Privacy Act, Personal Information (PI) as defined in the State of Alaska Personal Information Protection Act (APIPA), and Payment Card Information (PCI) as defined by Payment Card Industry Data Security Standard (PCI DSS), and Criminal Justice Information (CJI) as defined by the Federal Bureau of Investigation.

#### **3.7.4.1 Requirement**

The Offeror's proposed solution must include, define how they will ensure all sensitive, confidential, and/or restricted data is encrypted in-transit and at-rest. Criminal Justice Information Systems (CJIS) and those systems requiring MARS-E compliance must meet these encryption requirements using a FIPS 140-2 certified product.

DFCS owns the data and can demand it at any time. Proposed solutions that leverage public or private data sources resulting in DFCS business decisions – especially where the business decision reflects a DFCS legal jurisdiction related to due process – must ensure DFCS retains access to all the data required to support the decision.

#### **3.7.4.2 Requirement**

The Offeror's proposed solution must include, define, and validate the capabilities to return DFCS owned data to DFCS.

*Recovery Point Objective (RPO)* refers to the maximum amount of data loss – typically defined in terms of time – that may occur in the event of a system failure and consequent rollback to a known consistent state. *Recovery Time Objective (RTO)* refers to the maximum time that may pass between the point in time when a system failure occurs and the point in time when the system is recovered.

#### **3.7.4.3 Requirement – Recovery Point and Recovery Time Objectives**

The Offeror's proposed solution must include and define RPO and RTO capabilities. If there are cost-add RPO and RTO capabilities available that exceed the assumptions, scope and cost of your proposal, please identify those options.

### **3.7.5 Integration Security Controls**

When system interfaces (data exchange between systems) and integration requirements exist for a system, integration security controls must be documented and implemented to ensure the confidentiality, integrity and availability of the data for all valid business consumers. To simplify the

DFCS operating environment, and ensure that many of the required controls are met at the least cost, DFCS has implemented an Enterprise Service Bus (ESB) and partnered to leverage the Alaska Health Information Exchange (HIE). Both the ESB and the HIE provide architectural system integration and data exchange services that can be leveraged for re-use by On-DFCS premise and Off-site hosted information systems.

**3.7.5.1 Requirement**

The Offeror must demonstrate leveraging existing DFCS security control investments by integrating with DFCS systems via the DFCS ESB and/or the statewide HIE.

The Offeror must complete and submit to the DSO for review, one Interface Risk Assessment Worksheet, per interface, outlining the specifications and security components of said interface.

**3.7.6 DFCS Managed Off-site Hosting Considerations**

All DFCS Information Security Compliance and Privacy Services and Standards apply to DFCS managed off-site hosting scenarios.

**3.7.6.1 Requirement**

The Offeror must understand and acknowledge 3.7.6.

**3.7.7 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios**

DFCS IT expects that, by owning ongoing maintenance and technical operations, SaaS/XaaS solutions implicitly provide a limited degree of freedom to deviate from DFCS IT Information Security Compliance and Privacy Services and Standards. Specifically, when federal funding rights do not apply, and when DFCS is not performing technical services administration within the SaaS/XaaS hosting environment. SaaS/XaaS solutions may employ non-compliant infrastructure and non-compliant platform components in their design and implementation provided those infrastructure and platform components meet the security compliance requirements of the information managed by the SaaS/XaaS, and if applicable, the requirements in the DFCS Business Associate Agreement.

The Offeror's SaaS/XaaS proposal should include encrypting and securing any confidential data, and adopting the latest security measures available to prevent unauthorized access. Security controls include patching application/operating system/firmware, minimizing administrative controls, and completing a DFCS Authorization Package and submitting the Authorization Package to our department security office for review and approval, per the requirements under section 3.7.2. The authorization package must be approved before systems or applications are authorized for production. The Offeror assumes the responsibility for any and all authentication and account creations or modifications.

**3.7.7.1 Requirement – SaaS/XaaS Security Responsibilities**

Proposals for SaaS/XaaS offerings should include a clear delineation of the system's security mechanisms and configurations the Offeror will be responsible for, and those for which DFCS will be responsible.

The Offeror is also responsible for service patching and completing an RSA Authorization Package.

**3.7.7.2 Requirement – SaaS/XaaS Logging and Auditing**

For proposals that include SaaS/XaaS solutions that may manage confidential data, the SaaS/XaaS must include a logging and auditing solution. All components and systems within the Offeror's proposal are required to be capable of logging all data access requests to read or write data, including the requesting user id. The

audit-log data that is produced by the application must include all the data to identify who created, accessed, updated, and deleted data and when each event occurred.

The application must be readily capable of generating logging and auditing reports in a concise summary that can be easily subject to research by indexing. The industry standard solution the Offeror chooses to implement must be described, including how responsible DFCS entities (DSO, Division Data Owner) will be able to access it to perform oversight related tasks.

### **3.8 Enterprise Desktop and Mobility Services and Standards**

Enterprise Desktop and Mobility Services include the activities DFCS ITS performs to define, deploy, and support the DFCS enterprise desktop and mobility endpoints. DFCS maintains an enterprise desktop for all datacenter and field-deployed hosts. The desktop is based on a golden image, created and maintained based on input from the integration and development, information security, and operations service lines and standards. This section describes the procurement relevant enterprise desktop services and standards used to manage and maintain DFCS end-user desktops.

#### **3.8.1 Desktop Access and Configuration**

DFCS utilizes Dell workstation and server hardware. Offerors should propose solutions that are device independent. The DFCS Enterprise Desktop is a supported version of Microsoft Windows, with the supported web browser, productivity suite and other common, standard or approved software components and applications. See IT Reference D for currently supported hardware and operating system(s).

DFCS is a least privilege environment and staff are not granted elevated privilege without individually reviewed and approved security policy waivers. DFCS Program staff work with DFCS ITS to request, review, and determine compatibility, redundancy, and fit of non-standard software. DFCS Program staff are not permitted to install, nor can they independently authorize the installation of, new software components or applications on the desktop. Offerors should avoid solutions that require customization of the DFCS Enterprise Desktop.

If the Offeror's proposed solution requires use of a desktop web browser, the solution must be browser independent and be fully capable of functioning with the standard browser in the DFCS Enterprise Desktop Standards. See IT Reference D for currently supported web browser version(s).

If the Offeror's proposed solution requires use of desktop productivity suite software, the solution should be fully capable of functioning with the standard desktop suite in the DFCS Enterprise Desktop Standards. See IT Reference D for currently supported desktop productivity software.

##### ***3.8.1.1 Requirement – Desktop Access and Configuration***

The Offeror must propose a solution that supports the DFCS currently deployed desktop operating system (OS) and does not require elevated privileges for the end-user on their desktop. The Offeror must include activities in their proposal to establish whether each and every end-user desktop software component required to support the proposed solution is a part of the standard DFCS Enterprise Desktop. The Offeror must include activities in their proposal to work with the DFCS Enterprise Desktop team to integrate each non-standard software component. These activities must include working with DFCS Enterprise Desktop service line staff to:

- Accept or identify acceptable alternatives for each non-standard software component.
- Establish installation, configuration, and support procedures for each non-standard software component.

**3.8.1.2 Requirement – Web Browser Compatibility**

The Offeror must plan to support proposed solution compatibility with DFCS' currently deployed web browser version(s). The required functionality of the solution must be fully supported, or the Offeror must include in their proposal the plan, cost, and activities to make the proposed solution fully supported. The Offeror must review the DFCS standard browser vendor's support lifecycle material, published at the time of proposal. The Offeror's proposal must include a plan to migrate or upgrade any browser versions that will become unsupported during the execution of the contract (per the vendor's published support lifecycle material).

**3.8.1.3 Requirement – Desktop Productivity Software Compatibility**

The Offeror must plan to support DFCS currently deployed desktop productivity suite version(s). The Offeror must review the DFCS standard desktop productivity suite vendor's support lifecycle material, published at the time of proposal. The Offeror's proposal must include a plan to migrate or upgrade any versions of productivity suite software versions that will become unsupported during the planned execution of the contract (per the vendor's published support lifecycle material). The Offeror must include in their cost proposal, the optional contingency cost of one unanticipated productivity suite software version compatibility upgrade for the proposed application.

**3.8.1.4 Requirement – Other Desktop Software and Components**

The Offeror must delineate all the desktop software, access, and configuration requirements of the application not addressed elsewhere in the Enterprise Desktop Services and Standards section.

**3.8.2 Mobile Devices and Tablets**

Mobile devices for DFCS are:

- Dell Windows based Tablets
  - Configured with the latest version of Microsoft Standard browsers
  - Web applications are to be Browser version independent which means they support current versions of Internet browsers for Microsoft, FireFox, and Google Chrome.
  - Software should not be dependent on a specific version of MS Office Suite.
    - We move the organization as a whole during Department wide upgrades.
- Apple iOS based Tablets and Smart Phones
  - Configured with the latest version of Safari and Google Chrome.
  - Software should not be dependent on a specific version of MS Office Suite.
    - We move the organization as a whole during Department wide upgrades.

Dell and Apple Devices are configured with the latest operating systems or 1 version previous.

The DFCS mobile device strategy is evolving rapidly and is not stable or complete for supporting the ability to store or transmit confidential data. If their solution includes mobile device end-points, Offerors should plan for extensive engagement with the DFCS Enterprise Desktop and Mobility service line

**3.8.2.1 Requirement**

The Offeror must plan appropriate activities to support mobile device endpoint integration. These activities must include selecting and adapting mobile solution software components to a DFCS standard mobile device that supports all security compliance requirements of the data being stored on or transmitted to/from the mobile device endpoints.

**3.8.3 DFCS Managed Off-site Hosting Scenarios**

All DFCS Enterprise Desktop and Mobility Services and Standards apply to DFCS desktops managed off-site hosting scenarios.

**3.8.3.1 Requirement**

The Offeror must understand and acknowledge 3.8.3.

**3.8.4 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios**

DFCS IT expects that, by owning ongoing maintenance and technical operations, SaaS/XaaS solutions implicitly provide a limited degree of freedom to deviate from DFCS ITS Systems Operations and Administration Services and Standards. Specifically, when federal funding rights do not apply, and when DFCS is not performing technical services administration within the SaaS/XaaS hosting environment, SaaS/XaaS solutions may employ embedded, non-compliant, end-user desktops within the SaaS/XaaS, provided that:

- (a) Equivalent desktop security controls are proposed and implemented to those present on the DFCS Enterprise Desktop, and
- (b) The SaaS/XaaS supports DFCS Enterprise Desktop supported standard software for accessing SaaS solution desktops. See IT Reference D for supported software.

**3.8.4.1 Requirement**

When federal funding rights apply, *see section 3.4.4*, the Offeror's proposed solution must employ DFCS ITS Enterprise Desktop Services and Standards compliant platform components. This requirement supports State of Alaska operational risk mitigation in the event the Offeror determines to discontinue the service at a future date, and DFCS must assume maintenance and/or operations. If the Offeror cannot meet this requirement, they may propose an operational contingency statement the State of Alaska can consider as a viable risk mitigation alternative to assuming the future operational risks.

**3.9 DFCS Hosting and Datacenter Services and Standards**

DFCS Hosting and Datacenter Services include the activities DFCS ITS performs to design, implement, and operate standard information technology infrastructure and platform offerings in DFCS managed datacenters. This includes both the primary DFCS data centers in Juneau and Anchorage, as well as satellite facilities in secondary locations that require similar services to meet disaster recovery and business continuity requirements. Relying on robust, appliance style hardware with advanced storage area network data deduplication and replication functions, advanced firewalls, and virtualized host infrastructure, DFCS datacenter infrastructure provides the flexibility to rapidly deploy new hosts in a physically and logically secure environment.

Please see the DFCS Hosting and Datacenter Service Standards section of Reference D - Information Technology Standards,

**3.9.1 On-DFCS Premise Hosting Considerations**

DFCS provides and maintains a standardized set of infrastructure and platform services to deliver a full-service private cloud offering, leveraging the State of Alaska Wide Area Network to span two georedundant data centers located in Juneau and Anchorage.

**3.9.1.1 Requirement**



Proposals for hosting the solution on the State network should include the responsibilities and communication process for DFCS IT for development, test, and production environments and follow DFCS directives for migration to production.

The Offeror will not have direct access to the production environment on the State Network and must work through the appropriate protocols to effect change appropriately. The Offeror must work with DFCS IT for all security mechanisms, including patching updates.

**3.9.1.2 Requirement**

The Offeror will use the software identified in IT Reference D for the hosting of this application. The Offeror must state which version the application components are implemented in and how this solution will be accessed in the DFCS environment. The Offeror will need to identify what skills and expertise would be needed to support the proposed infrastructure.

**3.9.2 DFCS Managed Off-site hosting considerations**

All DFCS Hosting and Datacenter Services and Standards must be followed and applied to DFCS managed off-site hosting scenarios.

**3.9.2.1 Requirement**

The Offeror must understand and acknowledge 3.9.2.

**3.9.3 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios**

DFCS Hosting and Datacenter Services and Standards do not support Software as a Service (SaaS) or Anything as a Service (XaaS) offerings. Offerors proposing SaaS/XaaS solutions must provide and manage their own hosting and datacenter services. Offerors may subcontract these hosting and datacenter services, provided appropriate security agreements, such as a Business Associate Agreement or data usage agreement, are in place for the data being stored in or transported to/from the subcontracted hosting datacenter.

**3.9.3.1 Requirement**

The Offeror must understand and acknowledge 3.9.3.

**3.10 DFCS Wide Area Network, Telecommunications, and Perimeter Security Services and Standards**

DFCS Wide Area Network, Telecommunications and Perimeter Security Services include the activities DFCS IT performs to integrate the DFCS LAN with the State of Alaska (SOA) wide area network, telecommunications and perimeter security managed by Department of Administration (DOA) Office of Information Technology (OIT). These services are built upon a layered architecture design that includes VPN, ingress/egress, network address translation and port address translation services and capabilities provisioned, managed, and maintained by OIT. To maximize the security capabilities of these services and ensure systems maintain compliance with system security requirements and industry standards, DFCS ITS and OIT follow strict change management processes that include reviews and approvals for all information systems and applications changes that impact WAN, Telecommunications, and Perimeter Security. See 3.7 Information Security Compliance and Privacy Services and Standards for additional details regarding security compliance. Work and service requests reflecting these changes are managed via an OIT ticketing system (Reference D, section DFCS Wide Area Network, Telecommunications and Perimeter and WAN Security Service Standards).

### **3.10.1 State WAN and Bandwidth**

The State Wide Area Network (WAN) is maintained at the enterprise level by the Department of Administration (DOA)/Office of Information Technology (OIT); WAN connectivity and bandwidth available to grantees via the WAN is controlled by contractual agreements between OIT and local internet providers. Some rural areas experience internet connection speed as low as 56k and frequent network disruptions. Changes to the State WAN, for example new ingress points, IPSEC tunnels, etc., require both DFCS IT Security Office and DOA State Security Office review and approval.

Due to the great distances between communities in Alaska and the lack of road connections in most areas of the state, electrical power is locally generated in most parts of the state. While Anchorage has redundant transmission lines from its electrical generating plant and rarely experiences system-wide outages, local outages can occur due to weather-related conditions or damage to the distribution system. Electrical power in most other parts of the state is subject to periodic system-wide outages as well as localized outages. Broadband service is available in most of the larger communities in Alaska. However, in communities located off the road system that rely on satellite connections, a T1 line is a significant expense.

#### **3.10.1.1 Requirement**

The Offeror must understand and acknowledge Bandwidth constraints and denote any performance degradation that could be encountered by their solution and suggested mitigations. Offeror must note any services requiring communications outside the State of Alaska WAN.

### **3.10.2 DFCS Managed Off-site Hosting Scenarios**

DFCS operates only within the State of Alaska Wide Area Network and uses only State of Alaska provided telecommunications services. Proposals requiring new State of Alaska Wide Area Networks or telecommunications (phone, fax, etc.) services must be approved by the OIT Department Technology Officer.

#### **3.10.2.1 Requirement**

The Offeror must understand and acknowledge 3.10.2.

### **3.10.3 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios**

Offerors proposing SaaS/XaaS solutions must provide and manage their own Wide Area Network and telecommunications services to support any required network and telephony services of the proposed solution. The proposed solution must grant access to the DFCS Program staff via a supported DFCS desktop web-browser, or a desktop thin client, or similar DFCS approved and supported software. See Reference D - Information Technology Standards.

#### **3.10.3.1 Requirement**

The Offeror must understand and acknowledge 3.10.3.

## **3.11 Accessibility**

Alaska Administrative Orders 262 and 129 establish the Americans with Disabilities Act (ADA) compliance program in accordance with the American with Disabilities Act (42 U.S.c. 12101 et seq.). DFCS expects the Offeror to propose and deliver solutions that meet the Alaska ADA program.

### **3.11.1 ADA Compliance for Access to Information Systems and Applications**

DFCS requires ADA compliant application access.

Two important resources provide guidance for web developers designing accessible web pages. One is the Section 508 Standards, which Federal agencies must follow for their own new web pages. To learn more about the Section 508 Standards the Access Board maintains information on its website at [www.access-board.gov](http://www.access-board.gov).

The second is the General Services Administration information for web developers interested in accessible web design at <https://www.gsa.gov/technology/build-websites-and-digital-services>. This information was developed in conjunction with the Access Board, the Department of Justice, and the Department of Education

A more comprehensive resource is the Web Content Accessibility Guidelines developed by the Web Accessibility Initiative. These guidelines help designers make web pages as accessible as possible to the widest range of users, including users with disabilities. The Web Accessibility Initiative is a subgroup of the World Wide Web Consortium — the same organization that standardizes the programming language followed by all web developers.

Information for web developers interested in making their web pages as accessible as possible, including the current version of the Web Content Accessibility Guidelines (and associated checklists), can be found at <https://www.w3.org/WAI/standards-guidelines/wcag/>.

#### **3.11.1.1 Requirement**

DFCS requires that web pages and web applications be accessible for ADA compliance. This includes online forms and tables which must be made so that those elements are accessible. Documents on the website must be provided in HTML or a text-based format in addition to any other formats.

It is the responsibility of the Offeror to ensure that the web page\web application features are ADA compliant.

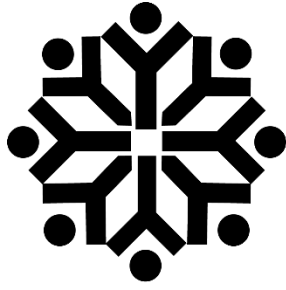
### **3.12 State of Alaska DFCS MITA Standards and Department IT Technology Standards**

The Department is migrating toward an enterprise Service Oriented Architecture (SOA) consistent with Medicaid Information Technology Architecture (MITA) and the Centers for Medicare and Medicaid Services (CMS) Seven Conditions and Standards (7C&S) outlined below:

- Modularity
- MITA Condition
- Industry Standards Condition
- Leverage Condition
- Business Results Condition
- Reporting Condition
- Interoperability Condition

#### **3.12.1 MITA Requirements**

The Offeror's proposal must respond to the questions on how their solution addresses or does not address each of the 7C&S.



**AK | DFCS**  
ALASKA DEPARTMENT OF  
FAMILY AND COMMUNITY  
SERVICES

## **Reference F**

# **Data Destruction Information and References**

State of Alaska  
Department of Family and Community Services

This is an overview of the State of Alaska and Federal Sources data destruction requirements for confidential information, as applicable to the State of Alaska, Department of Family and Community Services (DFCS). The department recognizes confidential information, information that identifies or could identify an individual, as personally identifiable information (PII) as defined in OMB Memorandum M-07-1616.

PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual. (GSA.gov)

A DFCS applicable example of this would be a data set that includes an individual's name and one other identifier such as, a social security number, date of birth, driver's license number, account number, password, employee id, or other access codes.

There are many laws and regulations defining PII. Here are just a few examples:

- Alaska Personal Information Protection Act (APIPA)
- Electronic Protected Health Information (ePHI)
- Personally Identifiable Information (PII)
- Criminal Justice Information (CJI)
- Criminal History Record Information (CHRI)

To meet the department's required standards for destruction of Electronic Protected Health Information (ePHI), Personally Identifiable Information (PII), Criminal Justice Information (CJI), or Criminal History Record Information (CHRI) staff must comply with the most current NIST guidance (currently NIST Special Publication 800-88 Revision 1). (Kissel, Regenscheid and Scholl) As outlined in NIST Special Publication 800-88 Revision 1, Appendix A—Minimum Sanitization Recommendations, DFCS requires that staff comply with the appropriate Clear, Purge, or Destroy mechanisms for all media. Additionally, Alaska Statute 45.48 (State of Alaska) Section 45.48.500 -.590 addresses the Disposal of Records by stating:

When disposing of records that contain personal information, a business and a governmental

agency shall take all reasonable measures necessary to protect against unauthorized access to or use of the records.

Notwithstanding (a) of this section, if a business or governmental agency has otherwise complied with the provisions of AS 45.48.500 — 45.48.590 in the selection of a third party engaged in the business of record destruction, the business or governmental agency is not liable for the disposal of records under AS 45.48.500 — 45.48.590 after the business or governmental agency has relinquished control of the records to the third party for the destruction of the records.

A business or governmental agency is not liable for the disposal of records under AS 45.48.500 — 45.48.590 after the business or governmental agency has relinquished control of the records to the individual to whom the records pertain.

In the HIPAA Disposal FAQ (HHS.gov) the Department of Family and Community Services and Human Services reiterates that PHI must be sanitized using specific means; see:

For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

Additionally, the HIPAA Security Series – Topic 3, Security Standards: Physical Safeguards (HHS.gov), outlines the following criteria for device reuse:

Are policies and procedures developed and implemented that address disposal of EPHI, and/or the hardware or electronic media on which it is stored?

Do the policies and procedures specify the process for making EPHI, and/or the hardware or electronic media, unusable and inaccessible?

## References

GSA.gov. <https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act>. 12 01 2020. Web. 19 02 2020.

HHS.gov. <https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html>. 18 02 2009. Web. 19 02 2020.

—. <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf>. 03 2007. Web. 19 02 2020.

Kissel, Richard, et al. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>. 12 2014. Web. 19 02 2020.

State of Alaska. <http://www.akleg.gov/basis/statutes.asp#45.48>. 2019. Web. 19 02 2020.