



October 7, 2020

**Request for Quote (RFQ) 20-0029458
Hewlett Packard Enterprise (HPE) Datacenter Care Renewal for Operational Support
Services**

You are invited to review and respond to this Request for Quote (RFQ) for Information Technology (IT) Services, entitled **Request for Quote (RFQ) 20-0029458, Hewlett Packard Enterprise (HPE) Datacenter Care Renewal for Operational Support Services**. In submitting your quote, you must comply with the instructions found herein. Please provide pricing through the terms of this contract by the Submission of Quotes date and time as noted on the Key Action Dates in Section I.3.

ALL QUOTES MUST BE SIGNED AND DATED PRIOR TO SUBMISSION.

Respondent must mail or deliver **one (1)** original, **one (1)** additional hardcopies, and **one (1)** electronic copy on CD/DVD-ROM or flash drive of your quote clearly labeled to the Department Contact named below. Neither e-mail submittals, nor fax transmittals will be accepted for this RFQ.

Delivery of all quote packages, including hand-delivered quotes and parcel post services, to the security desk located on the second floor. Please inform the security desk that you are dropping off a quote package. Quotes must be submitted under sealed cover, which must be plainly marked on the front of your package with your firm name and address and marked **“CONFIDENTIAL QUOTE - DO NOT OPEN Request for Quote (RFQ) 20-0029458, Hewlett Packard Enterprise (HPE) Datacenter Care Renewal for Operational Support Services.”**

Department Contact:

Brian Ito
California Department of Technology
Acquisition and IT Program Management Branch
(916) 431-5094
Brian.Ito@state.ca.gov

Hand Delivered or Parcel Post (UPS, FedEx, etc.)

California Department of Technology
Attn: Brian Ito
10860 Gold Center Dr., Suite 200 – Security Desk
Rancho Cordova, CA 95670

United States Postal Service (USPS)

California Department of Technology
Attn: Brian Ito
P.O. Box 1810, Mail Stop Y-18
Rancho Cordova, CA 95741-1810

Award of contract, if made, will be to the responsive, responsible respondent having the lowest total cost. Failure to adhere to the RFQ specifications may be considered a material deviation from the requirements of this RFQ, and may cause the quote to be rejected. This solicitation is being let under the delegated purchasing authority for IT goods and services governed by Public Contract Code (PCC) section 12100.

State Terms and Conditions and Bidder's Instructions applicable to this order are listed on the Department of General Services' (DGS) web sites listed below:

- DGS, Bidder's Instructions, revised 11/09/2011
<https://www.documents.dgs.ca.gov/dgs/fmc/gspd/gspd05-105.pdf>
- DGS, IT General Provisions GSPD-401IT, revised 09/05/14
https://www.documents.dgs.ca.gov/dgs/fmc/gspd/pd_401IT.pdf

TABLE OF CONTENTS

RFQ REQUIREMENTS

I.	<u>General Information</u>	
	1. Purpose.....	5
	2. Background.....	5
	3. Key Action Dates.....	5
	4. Written Questions.....	5
	5. Availability.....	6
	6. RFQ Response Guidelines.....	6
	7. RFQ Response Content.....	6
	8. Administrative Information.....	12
II.	<u>Evaluation Information</u>	
	1. Evaluation Process.....	14
	2. Evaluation Criteria.....	14
	3. Preference Programs.....	15
	4. Award and Execution.....	15
	5. Tiebreaker.....	15
III.	<u>Award and Protest Information</u>	
	1. Award of Contract.....	16
	2. Protests.....	16

EXHIBITS

<u>EXHIBIT A - Statement of Work</u>	18
<u>EXHIBIT A, Attachment 1 - Supplemental Data Sheet</u>	31
<u>EXHIBIT A, Attachment 2 - Capacity Commitment</u>	34
<u>EXHIBIT A, Attachment 3 - HPE Holidays</u>	35
<u>EXHIBIT A, Attachment 4 - Primary / Secondary / Local Support Hub Matrix</u>	36
<u>EXHIBIT A, Attachment 5 - Definitions</u>	37
<u>EXHIBIT A, Attachment 6 - Personnel Change Order Request Form</u>	39
<u>EXHIBIT A, Attachment 7 - Equipment List Template</u>	40
<u>EXHIBIT B – Payment and Invoicing</u>	41
<u>EXHIBIT B-1 – Cost Worksheet</u>	43
<u>EXHIBIT B-1A – Product Specifications: SAID # 1045 5828 9161</u>	44
<u>EXHIBIT B-1B – Product Specifications: SAID # 1045 5828 3945</u>	48
<u>EXHIBIT B-1C – Product Specifications: SAID # 1045 5976 9302</u>	63
<u>EXHIBIT C – General Provisions – Information Technology (GSPD-401IT) rev. 9/15/14</u>	67
<u>EXHIBIT D – Special Terms & Conditions to Safeguard Federal Tax Information</u>	68

EXHIBIT E – Security and Data Protection.....74

ATTACHMENTS

Attachment 1 – Administrative Requirements Checklist75

Attachment 2 – Security and Confidentiality Statement.....77

Attachment 3 – Payee Data Record, Std. 20478

Attachment 4 – Certification with the Secretary of State.....79

Attachment 5 – Civil Rights Laws Certification80

Attachment 6 – Pre-Employment Criminal Background Checks for Contractors.....81

Attachment 7 – Bidder Declaration Form.....82

Attachment 8 – Commercial Useful Function Certification83

Attachment 9 – Bidder Agreement to Technical Requirements84

SECTION I – GENERAL INFORMATION

1. PURPOSE

The California Department of Technology (CDT) is utilizing Hewlett Packard Enterprise (HPE) Datacenter Care Service to cover the current Windows equipment.

2. BACKGROUND

The California Department of Technology (CDT) needs to renew the existing Hewlett Packard Enterprise (HPE) Datacenter Care Service to cover the current Windows equipment. HPE Datacenter Care Service is HPE's most comprehensive support solution tailored to meet CDT's specific data center support requirements. It offers a wide choice of proactive and reactive service levels to cover requirements ranging from the most basic to the most business-critical environments. HPE Datacenter Care Service is designed to scale to any size and type of data center environment while providing a single point of contact for all CDT's support needs for HPE as well as selected multivendor products.

3. KEY ACTION DATES

Listed below are the key action dates and times by which specific actions must be taken or completed. If the CDT finds it necessary to change any of these dates, it will be accomplished by issuing an addendum.

KEY ACTION DATES	
Release of RFQ	10/7/2020
Submission of Written Questions	10/13/2020 @ 5:00 PM, PT
Response to Questions	10/14/2020
Last Day to Protest Requirements	10/15/2020
Submission of Quotes (by date and time)*	10/20/2020 @ 2:00 PM, PT
Evaluation*	10/20/2020
Notice of Intent to Award*	10/21/2020
Last Day to Protest Selection*	10/27/2020
Proposed Contract Execution Date*	10/28/2020

* All dates after the Submission of Quotes (by date and time) are approximate and may be changed without addendum to this RFQ to allow the CDT additional time for evaluation and contract execution.

4. WRITTEN QUESTIONS

All questions regarding the content of this RFQ must be submitted in writing via electronic mail (email) to the Department Contact named on the Cover Page of the RFQ and must be received by the date specified in Section I.3., Key Action Dates. Questions received after the date specified in Section I.3., Key Action Dates shall be answered at the State's option.

When the State has completed its review of the questions, all of the questions and answers will be distributed in writing to all the respondents via DGS Cal eProcure website: (<https://caleprocure.ca.gov/pages/>).

Please note: no verbal information given will be binding upon the State, unless such information is issued in writing as an official addendum.

5. AVAILABILITY

The selected respondent must be able to meet all requirements of this RFQ and be ready to begin offering their services and materials within ten (10) State business days of the contract award date specified in Section I.3., Key Action Dates, or the actual award date if later.

6. RFQ RESPONSE GUIDELINES

This RFQ and the respondent's quote in response to this document will be made a part of the Contract. Responses to this RFQ must contain all data/information requested and must conform to the format described in this RFQ. It is the respondent's responsibility to provide all required data and any other information deemed necessary for the CDT evaluation team to determine and verify the respondent's ability to perform the tasks and activities defined in the SOW, Exhibit A.

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

Unless otherwise specified, all electronic files and media submitted in response to this RFQ must be in formats compatible with the CDT's standard desktop computing environment, which consists of Microsoft (MS) Windows 7 SP 1, MS Office Suite 2010, and Adobe Acrobat Reader XI, et al.

7. RFQ RESPONSE CONTENT

The following documents must be submitted in the RFQ response, in the order specified below and will be reviewed for completeness as pass or fail. Any quote response that fails may be deemed non-responsive.

a. RFQ Response

The respondent must submit one (1) original copy of quote response, one (1) additional hard copies, and one (1) electronic copy on CD/DVD or flash drive.

b. Table of Contents

A table of contents that lists the response sections.

c. Cover Letter

The Bidder must include a cover letter signed by an individual who is authorized to bind the Bidder contractually. The cover letter must state that the individual is so authorized and must identify the title or position that the individual holds in the Bidder's firm. An unsigned cover letter may cause the Final Bid to be rejected.

The Cover Letter must contain the following information:

- Signature of an individual authorized to bind the firm contractually, identifies the signer's title and stipulates the signature authority;
- Statement that the bid response is the Contractor's binding offer, good for 90 calendar days from Final Bid due date, as noted in Section I.3 Key Action Dates;
- Statement indicating that the Bidder has available staff with the appropriate skills to complete performance under the Contract for all services and provide all deliverables as described in this RFQ; and,
- Statement accepting full Prime Contractor responsibility for coordinating, controlling, and delivering all aspects of the Contract and any Subcontractors on their team.
- Statement indicating that the bidder agrees to the terms and conditions of this RFQ and accepting responsibility as the Prime Contractor if awarded the Agreement resulting from this RFQ.

d. Administrative Requirements Checklist (Attachment 1)

The respondent must complete the required attachment checklist to confirm that all items are contained with the RFQ.

e. Security and Confidentiality Statement (Attachment 2)

One individual authorized to bind the company must complete the Security and Confidentiality form and include it with their quote.

f. Completed Cost Worksheet (Exhibit B-1)

All costs shall be filled out by the respondent.

g. Payee Data Record, Std. 204 (Attachment 3)

The respondent is required to submit a Payee Data Record, Std. 204 listing their Taxpayer Identification Number.

h. Certification with the Secretary of State (Attachment 4)

If required by law, the Prime Contractor must submit a Certificate of Status from California Secretary of State (SOS), showing Prime Contractor is certified with the SOS to do business in the State of California.

Domestic and foreign Corporations, Limited Liability Companies (LLCs) and Limited Partnerships (LPs) must be registered with the California SOS to be awarded the Contract. The SOS Certificate of Status must be included with the response. The required document(s) may be obtained through the SOS, Certification and Records Unit at (916) 657-5448 or through the following website: <https://businesssearch.sos.ca.gov/>.

If the Respondent does not currently have this certification, the firm must be certified before a Contract award can be made, and must provide information in the RFQ response to support the status of its application to be certified to do business in the State of California.

For more information, refer to the SOS website at:

<http://www.sos.ca.gov/business/be/faqs.htm>.

i. California Civil Rights Certification (Attachment 5)

Effective January 1, 2017, the Unruh Civil Rights Act and the Fair Employment and Housing Act (also referred to as the Acts; see Public Contract Code section 2010) establishes restrictions against contracting with vendors that have policies or practices that violate the Acts.

Pursuant to Public Contract Code (PCC) 2010, a person that submits a bid or proposal or proposes to renew a contract with, a state agency in the amount of \$100,000 or more shall certify, under penalty of perjury, at the time the bid or proposal is submitted or the contract is renewed, all of the following:

- That they are in compliance with the Unruh Civil Rights Act (Section 51 of the Civil Code).
- That they are in compliance with the California Fair Employment and Housing Act (Chapter 7 (commencing with Section 12960) of Part 2.8 of Division 3 of Title 2 of the Government Code).
- Supplier discrimination policies:
 - (1) That any policy that they have against any sovereign nation or peoples recognized by the government of the United States, including, but not limited to, the nation and people of Israel, is not used to discriminate in violation of the Unruh Civil Rights Act (Section 51 of the Civil Code) or the California Fair Employment and Housing Act (Chapter 7 (commencing with Section 12960) of Part 2.8 of Division 3 of Title 2 of the Government Code).
 - (2) Any policy adopted by a person or actions taken thereunder that are reasonably necessary to comply with federal or state sanctions or laws affecting sovereign nations or their nationals shall not be construed as unlawful discrimination in violation of the Unruh Civil Rights Act (Section 51 of the Civil Code) or the California Fair Employment and Housing Act (Chapter 7 (commencing with Section 12960) of Part 2.8 of Division 3 of Title 2 of the Government Code).

Respondents must complete and sign Attachment 5, California Civil Rights Laws Certification and submit with their bid response. Bidders must also agree to re-certify if the option to extend or an amendment to add time or funding to the contract is utilized.

j. Pre-Employment Criminal Background Checks for Contractors (Attachment 6)

- (1) The CDT recognizes the need for hiring practices that will ensure the greatest degree of security for data center operations and the data maintained within the Department. Under the authority of Government Code 11546.6, a criminal background check utilizing California Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) records must be conducted by the vendor on prospective contractors, subcontractors, volunteers, or vendors. All fingerprints shall be taken digitally using Live Scan technology and transmitted electronically to the DOJ. All costs associated with the fingerprinting processing is the responsibility of the prospective vendor.
- (2) The CDT retains the rights to conduct its own background check at a later time, if deemed necessary.
- (3) Vendor must submit a signed Attachment 6, Pre-Employment Criminal Background Investigation Policy Certification with their response certifying that upon award of contract, Contractor will comply with the Policy. Failure to provide the certification will result in disqualification or contract termination.

k. Disabled Veteran Business Enterprise (DVBE) Program Requirements

The DVBE Participation Requirements for this RFQ have been waived, but the CDT opts to include the DVBE Incentive. See DVBE Incentive below.

l. DVBE Incentive

In accordance with Section 999.5(a) of the Military and Veterans Code (MVC) an incentive will be given to respondents who provide DVBE participation. For evaluation purposes only, the CDT shall apply an incentive to quotes that propose California certified DVBE participation as identified on the Bidder Declaration GSPD-05-105, Attachment 8 and confirmed by the CDT.

For awards based on low price, the net quote price of the responsive quote will be reduced (for evaluation purposes only) by the amount of DVBE incentive as applied to the lowest responsive net quote price. If the #1 ranked responsive, responsible bidder is a California certified small business, the only bidders eligible for the incentive will be California certified small businesses. Incentive percentage is applied to cost points earned by the respondent. The following illustrates the incentive percentage available based on the respondent's confirmed percent of DVBE participation.

CONFIRMED DVBE PARTICIPATION OF	
5% and above	5%
4% - 4.99%	4%
3% - 3.99%	3%
2% - 2.99%	2%
1% - 1.99%	1%

m. Small Business Regulations

The Small Business (SB) regulations pursuant to the California Code of Regulations (Title 2, Division 2, Chapter 3, Subchapter 8, section 1896 et seq.) concerning the application and calculation of the SB preference, SB certification, responsibilities of SBs, department certification, and appeals can be viewed at (<http://www.dgs.ca.gov/pd/Programs/OSDS.aspx>). Access the regulations by Clicking on “Notice of Rulemaking” in the right sidebar. For those without Internet access, a copy of the regulations can be obtained by calling the DGS Office of SB and DVBE Services (OSDS) at (916) 375-4940.

n. Small Business Preference

The respondents claiming the small business preference must be certified by California as a small business. A 5% preference will be available to California certified SB. This preference must be claimed by completing the Bidder Declaration form GSPD-05-105, Attachment 7.

All certified SBs must perform a “commercially useful function” (CUF) in the performance of the contract, as defined in Government Code section 14837(d)(4). See CUF letter r of this section.

Certification applications and required support documents must be submitted to the OSDS no later than 5:00 p.m. on the RFQ due date; and the OSDS must be able to approve the application as submitted. Respondents may contact the OSDS for any information or questions concerning certification.

o. Non-SB Subcontracting Preference

A 5% preference is also available to a non-small business claiming 25% California certified SB sub-contractor participation. This preference must be claimed by completing the Bidder Declaration form GSPD-05-105, 9. The form must list all California certified SBs with which you commit to sub-contract with for an amount of at least 25% of the net contract price.

All certified SBs must perform a “commercially useful function” (CUF) in the performance of the contract, as defined in Government Code section 14837(d)(4). See CUF letter r of this section.

p. SB Nonprofit Veteran Service Agencies (SB/NVSA) Preference

SB/NVSA prime bidders meeting requirements specified in the MVC Section 999.5 et seq. and obtaining a California certification as a SB are eligible for the 5% SB preference. This preference must be claimed by completing the Bidder Declaration form GSPD-05-105, 9.

All certified SBs must perform a “commercially useful function” (CUF) in the performance of the contract, as defined in Government Code section 14837(d)(4). See CUF letter r of this section.

q. Bidder Declaration Forms (Attachment 7)

All respondents must complete the Bidder Declaration GSPD-05-105 form and include it with their quote response. When completing the declaration, the respondents must identify **all subcontractors** proposed for participation in the contract. The respondent awarded the contract is contractually obligated to use the subcontractors for the corresponding work identified, unless the CDT agrees to a substitution and it is incorporated by amendment to the contract. If no subcontractors are being utilized, please indicate none on the form.

The document and instructions may be accessed at the website link:

<https://www.documents.dgs.ca.gov/dgs/fmc/gspd/gspd05-105.pdf>.

Respondents who have been certified by California as a DVBE (or who are bidding rental equipment and have obtained the participation of subcontractors certified by California as a DVBE) must also submit a completed form(s) STD. 843 (Disabled Veteran Business Enterprise Declaration). All disabled veteran owners and disabled veteran managers of the DVBE(s) must sign the form(s). The completed form should be included with the quote response. Refer to the following website link to obtain the appropriate form:

https://www.documents.dgs.ca.gov/dgs/fmc/gspd/pd_843.pdf.

r. Commercial Useful Function Certification (Attachment 8)

If the Respondent or any Subcontractors are a California certified SB or DVBE, in accordance with AB 669 (Chapter 623, Statutes of 2003), the Respondent must address specific aspects of the legislation that requires to perform a CUF as defined by Government Code Sections 14837, 14838.6, 14839, 14842, and 14842.5.

A Respondent or subcontractor will not be considered to perform a CUF if the Respondent's or Subcontractor's role is limited to that of an extra participant in the transaction, the awarded Contract, or project through which funds are passed to obtain the appearance of SB or micro business participation.

Respondent must complete Attachment 8, CUF Certification. All Respondents and Subcontractors identified in the response to fulfill the requirements for one (1) or more of the socio-economic programs (DVBE and SB) must perform a CUF in the resulting contract. CUF is defined pursuant to MVC section 999(b)(5)(B) and Government Code section 14837(d)(4)(A) for the DVBE and small business programs, respectively.

If Respondent is not using Subcontractors, complete and sign Attachment with "Not Applicable". Failure to submit the requested written information as specified may be grounds for rejection.

s. TACPA Preferences

The following preferences will be granted for this procurement. Respondents wishing to take advantage of these preferences will need to review the following websites and submit the appropriate response with the quote:

- Target Area Contract Preference Act (TACPA)
<https://www.documents.dgs.ca.gov/dgs/fmc/pdf/std830.pdf>

Respondents wishing to take advantage of these preferences are required to submit the following applications/forms:

- TACPA (Std. 830)
- Respondent's Summary of Contract Activities and Labor Hours (DGS/PD 525)
- Manufacturer Summary of Contract Activities and Labor Hours (DGS/PD 526).

8. ADMINISTRATIVE INFORMATION

- a. The RFQ and the Respondent's response will be incorporated by reference into the resulting Contract.
- b. Upon Notice of Award posting, all documents submitted in response to this RFQ will become the property of the State of California, and will be regarded as public records under the California Public Records Act (PRA) (GC Section 6250 et. seq.) and subject to review by the public.
- c. Upon an executed Contract, the Contractor shall submit a signed Conflict of Interest, Statement of Economic Interest Form 700 (provided by the CDT Contract Administrator) for himself, his employees and any subcontractors assigned to this effort. This document is required by the Fair Political Practices Commission and further information is available at the following address: <http://www.fppc.ca.gov>.
- d. Prime Contractor's DVBE Subcontracting Reporting Requirements
- Military and Veteran Code (MVC) 999.5(d), Government Code (GC) 14841, and California Code of Regulations (CCR) 1896.78(e) requires all Prime Contractor's that had a Disabled Veteran Business Enterprise (DVBE) firm perform any element of work for a contract to report DVBE information.
- e. Federal Tax Administration Requirements

The CDT must notify the United States Internal Revenue Service (IRS) prior to executing, or amending, any contract to disclose, or provide access to, federal tax information (FTI) to a Contractor or Sub-Contractor, at least 45 calendar days prior to the disclosure of FTI, to ensure appropriate contractual language is included and that Contractors are held to safeguarding requirements. This procedure conforms to IRS Publication 1075, Exhibit 12 - 45-DAY NOTIFICATION REQUIREMENTS

f. Security and Data Protection Requirements

The CDT must ensure agreements with state and non-state entities include provisions which protect and minimize risk to the state when engaging in the development, use, or maintenance of information systems, products, solutions, or services. In order to comply with the State Administrative Manual (SAM) Section 5305.8, Bidders must comply with Exhibit E, Security and Data Protection.

g. GC 12990 and Non-Discrimination

Any employer who wishes to contract with the State for goods is subject to the provisions of GC 12990 relating to discrimination in employment. Contractors that do not meet the provisions of GC 12990 are not eligible to contract with the State for IT goods. Ineligible contractors are found in the California Regulatory Notice Register. To access the California Regulatory Notice Register, use this link: https://oal.ca.gov/california_regulatory_notice_online/

h. Plastic Trash Bag Certification Violations

Public Resources Code §42290 et seq. prohibits the State from contracting with any supplier, manufacturer, or wholesaler, and any of its divisions, subsidiaries, or successors that have been determined to be noncompliant to the recycled content plastic trash bag certification requirements. This includes award of a State contract or subcontract or renewal, extension, or modification of an existing contract or subcontract. Prior to award the State shall ascertain if the intended awardee or proposed subcontractor is a business identified on the current CalRecycle noncompliant list(s). In the event of any doubt of the status or identity of the business in violation, the State will notify the Board of the proposed award and afford the Board the opportunity to advise the State. No award will be made when either the bidder or a subcontractor has been identified either by published list or by advice from the Board, to be in violation of certification requirements.

SECTION II – EVALUATION INFORMATION

1. EVALUATION PROCESS

Each RFQ response will be checked for the presence of required information in conformance to the submission requirements of this RFQ. The CDT will evaluate each RFQ response to determine its responsiveness to the requirements. The CDT reserves the right to make mathematical corrections to cost worksheets and/or ask clarifying questions.

The overall responsiveness of each quote is based on the complete response from the respondent to the RFQ requirements, including the Statement of Work (SOW). An award, if made, will be to the responsive and responsible respondent providing the lowest cost accordance with Section II.B., Evaluation Criteria.

2. EVALUATION CRITERIA

The following two (2) sub-sections and criteria will be reviewed by the CDT’s evaluation team:

a. Administrative Requirements Evaluation (Pass/Fail)

Respondents must pass the Administrative Requirements Evaluation to continue on to the Cost Requirements Evaluation. All required attachments, forms, and documents as outlined below must be submitted.

ADMINISTRATIVE REQUIREMENTS		
1. 1 Master Copy of Quote Response and 1 Additional Copy		
2. 1 Electronic Copy of Quote Response on CD/DVD or Flash Drive		
3. Table of Contents		
4. Cover Letter		
5. Administrative Requirements Checklist (Attachment 1)		
6. Security and Confidentiality Statement (Attachment 2)		
7. Completed Cost Worksheet (Exhibit B-1)		
8. Payee Data Record, Std. 204 (Attachment 3)		
9. Certification with the Secretary of State (Attachment 4)		
10. California Civil Rights Certification (Attachment 5)		
11. Pre-Employment Criminal Background Checks for Contractors (Attachment 6)		
12. Bidder Declaration Forms (Attachment 7)		
13. Commercial Useful Function Certification (Attachment 8)		
14. Bidder Agreement to Technical Requirements (Attachment 9)		

ADMINISTRATIVE REQUIREMENTS (CONTINUED)		
1.	DVBE Incentive	<i>OPTIONAL</i>
2.	Small Business Preference	<i>OPTIONAL</i>
3.	Non-SB Subcontractor Preference	<i>OPTIONAL</i>
4.	SB Nonprofit Veteran Service Agencies (SB/NVSA) Preference	<i>OPTIONAL</i>
5.	TACPA Preferences	<i>OPTIONAL</i>

b. Cost Requirements Evaluation Criteria

If the RFQ response passes all Administrative Requirements, it shall be evaluated based on the Grand Total price as reflected on Exhibit B-1, Cost Worksheet.

3. APPLICATION OF OPTIONAL PREFERENCES AND INCENTIVE PROGRAMS

Cost adjustments for preference claims (TACPA and SB) and incentives (DVBE) will be performed during cost assessment.

4. AWARD AND EXECUTION

The basis of award shall be lowest evaluated cost. Contracts may be amended to exercise optional years or for additional funds (at the rates bid and evaluated). The State makes no guarantee as to the minimum or maximum usage of any one contract.

5. TIEBREAKER

In the event of a tie between lowest cost bidders, a coin toss shall be conducted in the presence of witnesses. Bidders will be invited to witness the coin toss, in addition state staff witnesses will also be present.

Note: In the event of a precise tie between suppliers claiming the incentive, the bid of an SB and the bid of a DVBE that is also a SB, the award shall go to the DVBE that is also an SB.

SECTION III – AWARD AND PROTEST INFORMATION

1. AWARD OF CONTRACT

Award of a contract, if made, will be to a single responsive and responsible respondent having the lowest total cost with all the requirements of the RFQ Section II – Evaluation, and any addenda thereto, except for such immaterial defects as may be waived by the State. The award will be made within forty-five (45) days after the scheduled date for Contract Award as specified in the RFQ; however, a respondent may extend the offer beyond 45 days in the event of a delay of contract execution.

The State reserves the right to determine the successful respondent(s) either on the basis of individual items or combination of all items included in its RFQ, unless otherwise expressly provided in the State's RFQ. Unless the respondent specifies otherwise in their quote, the State may accept any item or group of items of any quote. The State reserves the right to modify or cancel in whole or in part this RFQ.

Written notification of the State's intent to award will be made to all respondents who submit a quote. If a respondent, having submitted a quote, can show that their quote, instead of the quote selected by the State, should be selected for contract award, the respondent will be allowed five (5) working days to submit a protest to the Intent to Award, according to the instructions contained in the paragraph titled "Protests" of this RFQ.

2. PROTESTS

Any bidder's issues regarding solicitation requirements must be resolved (or attempts to resolve them must have been made) before a protest may be submitted according to the procedure below. These issues will first be resolved by the contact for the solicitation or if they result in a protest, the protest will be submitted to DGS Procurement Division Deputy Director to hear and resolve issues and whose decision will be final.

If a bidder has submitted a bid which it believes to be responsive to the requirements of the RFQ and to be the bid that should have been selected according to the evaluation procedures in the solicitation and the bidder believes the State has incorrectly selected another bidder for award, the bidder may submit a protest of the selection as described below. Protests regarding selection of the "successful vendor" will be heard and resolved by the Victim Compensation and Government Claims Board whose decision will be final.

All protests of award must be made in writing, signed by an individual authorized to bind the bidder contractually and financially, and contain a statement of the reason(s) for protest; citing the law, rule, regulation or procedure on which the protest is based. The protester must provide facts and evidence to support the claim. Protests must be mailed or delivered to:

Street and Mailing Address:
Deputy Director
Procurement Division
707 Third Street, Second Floor South
West Sacramento, CA 95605
Facsimile No.: (916) 375-4611

All protests to the RFQ or protests concerning the evaluation, recommendation, or other aspects of the selection process must be received by the DGS Procurement Division Deputy Director as promptly as possible, but not later than the date indicated in the Notification of Intent to Award and Key Action Dates in Section I. Certified or registered mail must be used unless delivered in person, in which case the protester should obtain a receipt of delivery.

Exhibit A: Statement of Work

1. Contract Description

Contractor's Name agrees to provide to the California Department of Technology (CDT), Hewlett Packard Enterprises (HPE), Datacenter Care (DC) Operational Support Services Agreement as described in this Statement of Work ("SOW"). All services described in this Agreement will be provided by the manufacturer HPE. HPE will perform the Services to support the equipment installed at CDT's datacenter location(s), as listed in Section 1.2 of this Statement of Work (SOW).

This Statement of Work ("SOW"), including any applicable exhibits or Attachments is effective as of the CDT Purchase Order (PO) issue date ("Effective Date"), and identifies the Datacenter Care Services ("Services") HPE will provide for the equipment located at California Department Technology's datacenter(s), as listed in Exhibit A, Attachment 2 and as further described below.

Handwritten or typewritten text (other than information specifically called for in the spaces provided) that purports to modify or supplement the printed text of this SOW shall have no effect and shall not add to or vary the terms of this SOW.

The Services to be performed by HPE are as follows:

- 2.1 Relationship Management Services
- 2.2 Enhanced Call Handling Services
- 2.3 Proactive Services
- 2.4 Reactive Support Services
- 2.5 HP Education Total One Service All Models

1.1. Contract Term

The term for these Services shall be for a period of 12 months. The scheduled start date is November 1, 2020 and will continue until October 31, 2021.

1.2. Equipment Site/Installation:

The "Equipment Site" shall mean the CDT's location, as identified in this Agreement, which is operated or controlled by CDT. Licensee may change the Equipment Site to another location located within the United States without incurring additional charges.

CDT, Office of Technology Services:

Gold Camp Campus 3101 Gold Camp Drive Rancho Cordova, CA 95670	Vacaville Campus 1020 Vaquero Circle Vacaville, CA 95688
--	--

1.3. Notices

All notices required by or relating to this Agreement shall be in writing and shall be sent to the parties of this Agreement at their address as set below unless changed from time to time, in which event each party shall notify the other in writing, and all such notices shall be deemed duly given if deposited, postage prepaid, in the United States mail and directed to the following addresses:

The technical representative during the term of this Agreement will be:

State Agency	Manufacturer
California Department of Technology Office Technology Services	Hewlett Packard Enterprises
Attn: Cary Yee	Attn: Claudia Garcia
Phone: (916) 228-6493	Phone: (916) 540-3109
E-mail: Cary.Yee@state.ca.gov	E-mail : Claudiagarcia@hpe.com

Contract inquiries should be addressed to:

State Agency	Contractor
California Department of Technology Acquisition & IT Program Management Branch	
Attn: Brian Ito	Attn:
Address: PO Box 1810 Rancho Cordova, CA 95741	Address:
Phone: (916) 431-5094	Phone:
E-mail: brian.ito@state.ca.gov	E-mail :

2. Scope of Work

2.1. Relationship Management Services

Datacenter Care Relationship Management includes HPE assigned account team who works with CDT to understand CDT business and IT objectives and provides the service delivery features described below. The HPE assigned account team provides these services, either remotely or on-site, at HPE's discretion, during the normal HPE business hours of Monday–Friday 8am–5pm Pacific Time Zone (PST) local time, excluding HPE holidays (See Exhibit A, Attachment 3: HPE Holidays).

Sections under Relationship Management Services include:

- a. Assigned Account Team
- b. Account Support Plan
- c. Support Planning and Review
- d. Support Activity Report

2.1.1. Assigned Account Team

The Assigned Account Team (AAT) is comprised of specific HPE personnel assigned to this

Datacenter Care Service and includes the following staff members:

1. HPE Datacenter Care Delivery Manager (DCDM)
2. HPE Account Support Manager (ASM)
3. Enterprise Services Manager (ESM)
4. Technical Account Manager (TAM)
5. Datacenter Hardware Specialist (DHS)

The AAT will assist CDT to address, and make recommendations regarding process or technology issues that could impact the CDT's Services. Working with CDT's technical staff and IT management, the AAT will provide advice and recommendations to assist CDT to manage its environment.

The ASM will be the single point of contact that oversees the delivery of the DC Services and will be responsible for coordinating the Proactive Services as set forth in this SOW.

The TAM will provide remote Proactive Services such as Support Planning and Review and Support-activity reporting services as set forth in this SOW.

The DHS will provide Proactive and Reactive Hardware Services as set forth in this SOW. The specific Deliverables of the AAT are set forth in this SOW.

2.1.2.Account Support Plan

At the beginning of the Services support period, a mutually agreed upon Account Support Plan (ASP) will be developed by the HPE ASM in conjunction with CDT's IT staff and the HPE AAT and will be documented via the Change Management and Work Authorization process. CDT agrees to provide, in a timely manner, knowledgeable resources to assist with the development of the Account Support Plan. The ASP documents the reactive and proactive support, devices, geographic coverage, and other support aspects provided by the Service. The account support plan also details roles and responsibilities, along with contact information and escalation procedures and will be completed with CDT as part of the startup phase of this service and routinely reviewed.

Any changes to the ASP will require the agreement of both parties.

2.1.3.Support Planning and Review

The ASM will coordinate and conduct monthly onsite support planning and review sessions of the Account Support Plan. During these reviews, CDT, the ASM, and the HPE Assigned Account team will review the support provided by HPE over the monthly period, including key topics arising from the Support-activity Report and the outcome of DC activities. These reviews provide an opportunity to discuss trends, any planned changes to CDT's IT environment and business, and the impact of these changes to CDT's support requirements. Any additional support requirements can also be identified and discussed and may be subject to the change management process.

These review sessions provide an open communication forum for CDT to share the organization's business and IT goals and to understand what changes, if any, to the Services may be needed throughout the term of this SOW. During the review sessions, the HPE AAT will share HPE best practices and provide IT operational and technical advice related to the current and future operational needs and projects. Members of the HPE AAT may participate in these meetings, as determined by the ASM. As a result of the review session, the Account Support Plan will be updated following the process stated in Section 2.1.2 Account Support Plan.

2.1.4.Support-Activity Report

The HPE TAM will create and provide CDT with a monthly Support-activity report that documents reactive support-call information during that specific period. If potential risk factors are identified, HPE will provide any recommendations for consideration by the CDT.

2.2. Enhanced Call Handling Services

Enhanced Call Handling is a set of integrated and accelerated reactive processes designed to address hardware and software incidents.

Sections under Enhanced Call Handling Services include:

- 2.2.1 Rapid Response to Critical Hardware and Software Incidents
- 2.2.2 Accelerated Escalation Management
- 2.2.3 Remote Hardware and Software Incident Diagnosis and Support
- 2.2.4 HPE Electronic Remote Support

2.2.1.Rapid Response to Critical Hardware and Software Incidents

HPE will provide CDT access to a dedicated HPE phone number 24 hours a day, 7 days per week. When a critical hardware or software incident (severity 1 or 2) occurs, CDT will be connected to a remote technical HPE support. The HPE support specialist is specialized in business recovery in complex computing environments and has access to information about CDT's IT environment, systems, and specific support requirements. In the event of a hardware issue that may require an onsite presence, a HPE hardware specialist will be dispatched to CDT's location in accordance with the hardware reactive service level of the affected device. Additionally, the HPE support specialist will perform failure data collection and incident definition. If necessary, the HPE support specialist will execute escalation procedures and engage additional technical specialists.

2.2.2.Accelerated Escalation Management

For critical incidents (severity 1 or 2), HPE will assign a Critical Event Manager (CEM). The CEM will coordinate incident escalation and will enlist other HPE specialists if the situation requires additional resources and skills.

2.2.3.Remote Hardware and Software Incident Diagnosis and Support

CDT will report hardware or software incidents (Severity 3 and 4) to HPE using one of three methods which are available 24 hours a day, 7 days per week:

- a. Dedicated HPE phone number
- b. HPE Electronic Remote Support as a web-based submittal tool via the HPE Support Center
- c. HPE Electronic Remote Support as an automated equipment reporting event
- d. HPE Software Support Online as a web-based submittal portal for HPE Software products

HPE will acknowledge the receipt of the service request by logging the call, assigning a case ID, and communicating the case ID to CDT. HPE will work during the hardware or software coverage window to isolate the problem and to remotely troubleshoot, remedy, and resolve the problem with CDT.

2.2.4. HPE Electronic Remote Support

The Electronic Remote Support tool provides troubleshooting and repair capabilities. CDT will have access to:

- a. Capabilities available to registered users such as the ability to download selected HPE firmware based on purchased software entitlement, to subscribe to hardware-related proactive service notifications, to participate in support forums, and to share best practices with other registered users
- b. Expanded Web-based searches of technical support documents
- c. Certain HPE proprietary service diagnostic tools with password access
- d. A web-based tool for submitting questions directly to HPE which allows for viewing and tracking the status of each support request submitted either through the tool or via the phone.
- e. HPE and third party hosted knowledge databases for certain third party products

2.3. Proactive Services

Sections under Proactive Services include:

- a. Server Operating System Patch Analysis and Management
- b. Firmware Analysis and Management

2.3.1. Server Operating System Patch Analysis and Management

For Microsoft operating systems:

- a. HPE will provide a written Microsoft Service Pack Briefing, which addresses the features of the latest Microsoft operating system and server application service packs.
- b. In addition, HPE will provide a yearly notification on Microsoft Security Releases and a yearly notification on HPE-Microsoft Supported Products, applicable to servers outlined in CDT's ASP.

For the Linux operating system, HPE will review Linux patch notifications from Linux suppliers (Red Hat and/or SUSE) and provide recommendations of for installation.

For VMware and Microsoft Hyper-V Hypervisors, HPE will review patch notifications from suppliers and provide recommendations of patches for installation.

2.3.2. Firmware Analysis and Management

Periodically, HPE and vendors for which HPE is an authorized service provider release firmware and related software updates for equipment. These updates may address potential incidents, provide added functionality or improve performance. On a quarterly basis, HPE will analyze for server firmware and related software updates for the equipment listed in Exhibit A, Attachment 2: Commitment Capacity. CDT and the HPE AAT will discuss recommended updates and update planning assistance.

For HPE firmware updates that are defined as non-CDT installable, HPE will install these updates, if requested by CDT at a mutually agreeable time. HPE will provide CDT telephone assistance for the installation of CDT-installable firmware if needed during the service coverage window.

2.4. Reactive Support Services

The equipment listed in Exhibit A, Attachment 2, requires a valid, active reactive support agreement provided by HPE and/or covered under warranty throughout the term of this SOW to be eligible for these services. If CDT purchases reactive support services for equipment under a separate agreement with HPE, CDT acknowledges and agrees to maintain that equipment under an active support agreement with HPE throughout the term of this SOW. If equipment is covered under warranty only, CDT agrees to purchase reactive support from HPE for the equipment upon expiration of the product warranty through the term of this SOW.

Decommissioned devices need 30 days' prior notice to be taken off the support contract and can be done via True Up process. The decommissioned items will not require break fix support. If reactive services are not provided under a separate agreement with HPE or provided under warranty, the reactive support services, as set forth in this SOW, will be provided for the equipment that will be entitled by HPE under this SOW. For equipment listed in Exhibit A, Attachment 2 that is entitled by HPE, either via an existing HPE reactive support agreement(s) and/or HPE warranty coverage, the reactive support services will be provided as defined by the existing agreement(s) and/or warranty coverage.

Sections under Reactive Support Services include:

- 2.4.1 Service Coverage Window
- 2.4.2 Hardware Reactive Support
- 2.4.3 Software Reactive Support
- 2.4.4 Software Product and Documentation Updates

2.4.1. Service Coverage Window

The Service Coverage Window specifies the time during which reactive services are delivered remotely or onsite. For CDT the coverage window is 24 hours per day, Monday through Sunday including HPE holidays.

Calls received outside the defined coverage window as defined on the reactive support agreement will be logged at the time the call is placed to HPE, but will not be acknowledged until the next coverage window commences.

2.4.2. Hardware Reactive Support

For the hardware products included in Attachment A, Exhibit 2: Initial Commitment Capacity, the hardware reactive support is a 4-hour onsite response with a 24x7 coverage window. An HPE authorized representative will arrive at CDT's site within 4 hours after the service request has been received and acknowledged by HPE.

For the hardware products covered via pre-existing HPE reactive support agreement or pre-existing HPE warranty coverage, the hardware reactive support will have a response and coverage window as defined in those separate agreements. Hardware covered under pre-existing agreements or warranties will be included in this Agreement via the True-Up Process upon expiration of those separate agreements.

For hardware incidents that cannot be resolved remotely, an HPE authorized representative will provide onsite technical support on covered hardware products to return them to operating condition. For certain products, HPE may, at its sole discretion, elect to replace such products in lieu of repairing them. Replacement products are new or functionally equivalent to new in performance. Replaced products become the property of HPE with exception of storage media/

hard drives. For the items kept by CDT, HPE will subject to additional charges.

At time of onsite technical support delivery, HPE may:

- a. Install available engineering improvements to help with proper operation of the hardware products and maintain compatibility with HPE-supplied hardware replacement parts
- b. Install available firmware updates defined by HPE as non-CDT installable that, in the opinion of HPE, are required to return the covered product to operating condition or to maintain supportability by HPE and for which CDT has the required license to use, if applicable.

Once an HPE authorized representative arrives onsite, the representative will continue to deliver the service, either onsite or remotely at the discretion of HPE, until products are repaired. Work may be temporarily suspended if additional parts or resources are required, but work will resume when they become available.

2.4.3. Software Reactive Support

Once a non-critical software incident (severity 3 or 4) is logged, HPE will respond to the call within 2 hours after the service request has been logged, if this time falls within the contracted Service Coverage Window. HPE will provide corrective support to resolve identifiable and CDT-reproducible software product problems. HPE will also provide support to help identify problems that are difficult to reproduce.

For a critical software incident (severity 1 or 2), please see Section 3.2 Enhanced Call Handling Services.

For a critical software incident (severity 1 or 2) for HPE Application Software products covered under HPE Software Enterprise Support, please see attached datasheets in Exhibit A, Attachment 1: Supplemental Data Sheet. SLOs begin after initial response from DC team.

2.4.4. Software Product and Documentation Updates

As HPE releases updates to HPE software, the latest revisions of the software and reference manuals will be available to CDT, corresponding to CDT's prerequisite underlying software license from HPE or third-party software vendor. For selected third-party software, HPE will provide software updates as such updates are made available from the third party, or HPE may provide instructions on how to obtain software updates directly from the third party. A license key or access code or instructions for obtaining a license key or access code, will be proved to CDT when required to download, install, or run the latest software revision.

For most HPE software and selected HPE-supported third-party software, updates will be made available through the Software Updates and Licensing portal via the HPE Support Center or the HPE Software Support Online portal. For other HPE-supported third-party software, CDT may be required to download updates directly from the vendor's website.

2.5. HP Education Total One Service All Models

HPE will provide Education and Training to State. The Scope of Education and Training will be agreed to in advance.

3. True-Up/Review Process

Contractor's Name will invoice CDT for the first monthly payment based on the equipment listed in Exhibit A, Attachment 2.

HPE will perform a review process for CDT equipment additions, deletions, and changes to Service levels. The review process may also include the review of Customer's forecast for Add-on Service for planned add-ons for hardware products and any additional invoicing and price adjustments required upon the annual review process. CDT will not be denied support on devices that are not in this SOW contract, but will be added on the following true up.

Changes for equipment deletions will require thirty (30) days advance notice. The price change will be effective from the date of deletion. A prorated credit will be on the next invoice.

Changes for equipment additions or to Service levels will require advance notice, in writing, before the Service levels will be available. The price change will be effective from the date of addition or change in Service level. A prorated amount and the next invoicing period amount for the Services will be on the next invoice.

Monthly payments will be based off a True-ups during that period. Contractor's name will be sent the True-up list on the 1st business day of each month.

HPE will attach the equipment list showing the current equipment covered, equipment added, equipment removed and individual cost for each line item. The equipment list will be based on the template listed in Exhibit A, Attachment 7: Equipment List Template.

4. Escalation Process

The parties acknowledge and agree that certain technical and project related problems or issues may arise, and that such matters shall be brought to the Department of Technology's attention. Problems or issues shall normally be reported in regular status reports. There may be instances, however, where the severity of the problems justifies escalated reporting. To this extent, the Contractor will determine the level of severity and notify the appropriate Department of Technology personnel. The Department of Technology personnel notified, and the time period taken to report the problem or issue, shall be at a level commensurate with the severity of the problem or issue. The Department of Technology personnel include, but are not limited to, the following:

- First level: Cary Yee, Hypervisor IT Manager I
- Second level: Richard Gillespie, Compute & Storage IT Manager II
- Third level: Scott MacDonald, Infrastructure Services Deputy Director

Contact the HPE CDT Solution Center (CSC)

Depending on the support level, there are different numbers in which to call.

- Warranty/Foundation Care/Proactive24 (P24) 800-633-3600
- Proactive Care (PC) 866-211-5211
- Critical Service (CS, CA) 888-761-7437
- Datacenter Care (DC) 888-751-2149

Provide the 10 digit Support Case number

Ask the agent to speak to the CSC Manager on Duty (MOD)

The CSC MOD will review the case to determine the best path forward on a resolution. The MOD can typically resolve the concern without having to escalate any further.

If the CSC MOD is unable to assist or additional follow-up is needed:

Contact a local HPE District Manager or the HPE Support Team Lead. If CDT is unable to contact the local HPE District Manager or the HPR Support Team Lead immediately on the phone, leave a detailed voice mail (or send an email) with the HPE support case number, company name, and contact information.

Please refer to the Account Support Plan (ASP) for CDT assigned HPE team information and tailored escalation procedures.

The parties acknowledge and agree that certain technical and project related problems or issues may arise, and that such matters shall be brought to the CDT's attention. Problems or issues shall normally be reported in regular status reports. There may be instances, however, where the severity of the problems justifies escalated reporting. To this extent, the Contractor will determine the level of severity and notify the appropriate CDT personnel. The CDT personnel notified, and the time period taken to report the problem or issue, shall be at a level commensurate with the severity of the problem or issue. The CDT personnel include, but are not limited to, the following:

- First level: Cary Yee, Hypervisor IT Manager I
- Second level: Richard Gillespie, Compute & Storage IT Manager II
- Third level: Scott MacDonald, Infrastructure Services Deputy Director

5. Vendor Personnel Change

The Contractor will notify the CDT, in writing, within five (5) calendar days of any changes in the personnel assigned to the project tasks/deliverables by completing a Personnel Change Order Request form, Exhibit A, Attachment 7 with attached resume and staff experience worksheet. If a Contractor employee is unable to perform due to illness, resignation, or other factors beyond the Contractor's control, the Contractor will make every reasonable effort to provide suitable substitute personnel. The substitute personnel must be equal or better qualifications than the replaced personnel, meet all requirements and be approved in advance of any performance under the Contract by the CDT Contract Administrator via an approved Personnel Change Order Request form.

6. Obligations, Limitations, and Assumptions

1. See Exhibit A, Attachment 1: Supplemental Data Sheet for additional general requirements and limitations.
2. Any Services not described in Section 2 are considered outside the scope of this SOW.
3. CDT will assign a Program sponsor and alternate for the duration of the delivery of the Program. This person will have signature authority, the authority to assign and direct the activities of CDT resources, and will be available to HPE personnel throughout the

term of the Program.

4. CDT will need to have assigned points of contacts that work directly with the ASM and DHS for critical failures. HPE will have that contact to reach for critical failures and in turn that resource can communicate with the CDT team; thus, eliminating duplicate support requests. As such, CDT will establish an internal communication plan for critical problems to ensure rapid resolution and clear communication on a peer-to-peer basis between HPE and CDT.
5. Services will be performed during HPE business working hours, Monday through Friday, 8:00 a.m. to 5:00 p.m. local time, excluding HPE holidays ("Standard Work Day") unless otherwise stated in this SOW. Weekend and holiday hours or hours outside the Standard Work Day may be available at an additional charge, and are subject to the Change Management Process of this document. Prior to work being performed outside the Standard Work Day, a completed Changed Order will be required with the approval of HPE.
6. Services will be performed at HPE offices and at CDT's location.
7. CDT will provide HPE access to CDT's locations, building facilities, computer room facilities, equipment, etc., as needed in performance hereunder. If security restrictions apply, CDT will be required to assist HPE personnel.
8. CDT will provide advance notice to HPE for any equipment changes to the equipment as listed in Exhibit A, Attachment 2. These changes may affect maintenance fees, parts sparing, or support requirements. CDT will use the Change Management process defined in Section 3, herein, to communicate the details for the equipment changes.
9. Authorization to Install Software. During delivery of Custom Support Services, HPE may be required to install copies of third-party or HPE Branded Software and be required to accept license terms accompanying such Software ("Shrink-Wrap Terms") on behalf of CDT. Shrink-Wrap Terms may be in electronic format, embedded in the Software, or contained within the Software documentation. CDT hereby acknowledges that it is CDT's responsibility to review Shrink-Wrap Terms at the time of installation, and hereby authorizes HPE to accept all Shrink-Wrap Terms on its behalf.
10. Documentation created for this Datacenter Care Service will be available in electronic format using Microsoft Office.
11. Assistance for step-by-step instruction for software installation and configuration is out of scope unless delivered as part of a HPE Proactive Select Service.
12. Performance tuning is out of scope unless delivered as part of a HPE Proactive Select Service.
13. Parts and components that have exceeded their maximum supported lifetime and/or the maximum usage limitations as set forth in the manufacturer's operating manual product quick-specs, or the technical product data sheet will not be provided, repaired, or replaced as part of this service. Items that reach End of Support Life will be documented in support contract and HPE will provide best effort to support this equipment.

14. HPE Hardware onsite response times are limited as follows (Exhibit A, Attachment 4 contains a matrix of the HPE Hub locations for the Northwest. Incident Severity Levels are defined in Exhibit A, Attachment 5: Definitions):

Distance from HPE designated support hub			
0-25 miles (0-40km)	2 hours	4 hours	Next coverage day
26-50 miles (41-80km)	Established at time of order and subject to availability	4 hours	Next coverage day
51-100 miles (81-160km)	Not available	4 hours	Next coverage day
101-200 miles (161-320km)	Not available	8 hours	1 additional coverage day
201-300 miles (321-480km)	Not available	Established at time of order and subject to resource availability	2 additional coverage days
Greater than 300 miles (481+km)	Not available	Established at time of order and subject to resource availability	Established at time of order and subject to resource availability

15. Upon HPE request or when CDT calls in for support, the CDT will be required to support HPE's remote problem resolution efforts by:
- Starting self-test and installing and running other diagnostic tools and programs
 - Installing CDT-installable firmware updates and patches
 - Providing all information necessary for HPE to deliver timely and professional remote support and to enable HPE to determine the level of support eligibility
 - Performing other reasonable activities to help HPE identify or resolve problems as requested by HPE
16. During the delivery of the Program, HPE will use the suite of remote support tools and technologies which provide for a wide range of proactive capabilities including continuous event monitoring, automatic collection of configuration and topology data and automated notification of potential problems. These tools allow HPE support technicians to execute remote troubleshooting and diagnostic tools, to understand equipment configurations, to identify configuration changes, and to analyze CDT's configuration against HPE standard best practices. Recognizing that any remote support solution must provide security for the CDT's IT environment, these HPE remote support technologies will comply with industry-standard security tools and practices and State of California policies/legislative mandates.
17. CDT is responsible for maintaining the contact detail configured in the remote support solution that HPE will use in responding to an equipment failure.
18. CDT is responsible for registering to use the HPE or a third- party vendor's electronic services in order to access knowledge databases and to obtain product information. HPE will provide registration information to the CDT for the HPE electronic services.
19. CDT is responsible for the security of its IT environment.

20. At HPE's discretion, service will be provided using a combination of remote diagnosis and support, services delivered onsite, and other service delivery methods. Other service delivery methods may include the delivery via a courier of CDT- replaceable parts such as a keyboard, a mouse, other parts classified as CDT Self Repair parts, or an entire replacement product, with exception of storage media/ hard drives,. HPE will determine the appropriate delivery method required to provide effective and timely support. The CDT will be responsible for returning the defective part or product within a time period designate by HPE.
21. HPE is not liable for the performance or non-performance of third party vendors, their products, or their support services. Purchase of any Collaborative Support Services does not assign the support agreement between the CDT and the third party vendor to HPE. The CDT is responsible for the performance of obligations under such third party agreements, including payment of all applicable fees, including any fees that may apply as a result of logging calls with the vendor.
22. The following list includes some, but not necessarily all, specific Services that are excluded from this Program:
 - a. Troubleshooting for interconnectivity or compatibility problems
 - b. Services required due to failure of the CDT to incorporate any system fix, repair, patch, or modification provided to the CDT by HPE
 - c. Services required due to failure of the CDT to take avoidance action previously advised by HPE
 - d. Services that, are required due to unauthorized attempts by non- HPE personnel to install, repair, maintain, or modify hardware, firmware, or software
 - e. Operational testing of applications or additional test requested or required by the CDT
 - f. Backup and recovery of the operating system, other software, and data
 - g. Services that, are required due to improper treatment or use of the products or equipment
 - h. Equipment installations, moves, additions, changes, de-installations, and disposal
 - i. Reconfiguration of equipment
23. For all servers included in the Services, the CDT is responsible for purchasing the operating system and related software support licenses from HPE or third party software provider. The CDT will retain and provide to HPE upon request all original software licenses, license agreements, license keys and subscription service registration information as applicable for this Program.
24. Software updates are not available for all software products. Upon the CDT's request, HPE will provide the list of software product families that currently do not include software updates.
25. For some products, software updates include only minor improved features. New software versions must be purchased separately. Upon the CDT's request, HPE will provide the list of software product families where entitlement to receive and use new versions of software is not included.
26. Multivendor Network Support:
 - a. CDT is responsible for purchasing network support agreements from HPE or a third-party vendor.
 - b. The following are excluded from Multivendor Network Support:

- 1) Establishment of a contract between the third-party vendor and the CDT
 - 2) Establishment of a service-level agreement concerning, or assumption of responsibility for, the performance of a third-party vendor's products or services
 - 3) Resolution or repair of third party equipment changes to restore solution to original operable state
 - 4) Subcontracting of any service to a third-party vendor, including billing that vendor on the CDT's behalf
 - 5) CDT is responsible for notifying the third-party network vendor appointing HPE as their special agent in order for HPE to contact the vendor.
27. HPE, at its discretion, may utilize HPE authorized partner or original equipment manufacturer (OEM) resources to deliver reactive services.

Exhibit A, Attachment 1: Supplemental Data Sheet

This Supplemental Data Sheet provides additional general requirements and limitations that apply to HPE's support offerings, which are set forth in detail in offering-specific datasheets with the exception of those support offerings delivered by HPE Software.

1. SERVICE ELIGIBILITY

Hardware Support-General Eligibility. Hardware products must be in good operating condition, as reasonably determined by HPE, to be eligible for placement under support. CDT must also maintain eligible products at the latest HPE-specified configuration and revision levels.

Return to Support. If CDT allows support to lapse, HPE may charge CDT additional fees to resume support or require CDT to perform certain hardware or software upgrades.

Use of Proprietary Service Tools. HPE may require CDT to use certain hardware and/or software system and network diagnostic and maintenance programs ("Proprietary Service Tools"), as well as certain diagnostic tools that may be included as part of the CDT system. Proprietary Service Tools are and remain the sole and exclusive property of HPE, and are provided "as is." Proprietary Service Tools may reside on CDT systems or sites. CDT may only use the Proprietary Service Tools during the applicable Support coverage period and only as allowed by HPE and CDT may not sell, transfer, assign, pledge, or in any way encumber or convey the Proprietary Service Tools. Upon termination of Support, CDT will return the Proprietary Service Tools or allow HPE to remove these Proprietary Service Tools. CDT will also be required to:

- Allows HPE to keep the Proprietary Service Tools resident on CDT systems or sites, and assist HPE in running them;
- Install Proprietary Service Tools, including installation of any required updates and patches;
- Use the electronic data transfer capability to inform HPE of events identified by the software;
- If required, purchase HPE-specified remote connection hardware for systems with remote diagnosis service; and
- Provide remote connectivity through an approved communications line.

2. SUPPORT LIMITATIONS

Local Availability of Support. Some offerings, features, and coverage (and related products) may not be available in all countries or areas. In addition, delivery of support outside of the applicable HPE coverage areas may be subject to longer response times, reduced restoration or repair commitments, and reduced coverage hours.

Version Support. Unless otherwise agreed by HPE in writing, and for those offerings not delivered by HPE Software, HPE only provides support for the current version and the immediately preceding version of HPE branded software, and provided that HPE branded software is used with hardware or software included in HPE-specified configurations at the specified version level. "Version" means a release of software that contains new features, enhancements, and/or maintenance updates, or for certain software, a collection of revisions packaged into a single entity and, as such, made available to CDT.

Relocation and impact on Support. Relocation of any products under support is CDT responsibility and is subject to local availability and fee changes. Reasonable advance notice to HPE may be required to begin support after relocation. For products, any relocation is also

subject to the license terms for such products.

Multi-vendor Support. HPE provides support for certain non-HPE branded products. The relevant data sheet will specify availability and coverage levels and the support will be provided accordingly, whether or not the non-HPE branded products are under warranty. HPE may discontinue support of non-HPE branded products if the manufacturer or licensor ceases to provide support for them.

Modifications. CDT will allow HPE, at HPE's request, and at no additional charge, to modify products to improve operation, supportability, and reliability, or to meet legal requirements.

3. CDT RESPONSIBILITIES

Site and Product Access. CDT will provide HPE access to the products covered under support; and if applicable, adequate working space and facilities within a reasonable distance of the products; access to and use of information, CDT resources, and facilities as reasonably determined necessary by HPE to service the products; and other access requirements described in the relevant data sheet. If CDT fails to provide such access, resulting in HPE's inability to provide support, HPE shall reschedule with CDT to gain access. CDT is responsible for removing any products ineligible for support, as advised by HPE, to allow HPE to perform support. If delivery of support is made more difficult because of ineligible products, HPE will charge CDT for the extra work at HPE's published service rates.

Licenses. CDT may purchase available product support for HPE branded products only if CDT can provide evidence that CDT have rightfully acquired an appropriate HPE license for the products, and CDT may not alter or modify the products unless authorized by HPE at any time.

Software Support Documentation and Right to Copy. CDT may only copy documentation updates if CDT purchased the right to copy them for the associated products. Copies must include appropriate HPE trademark and copyright notices.

Loaner Units. HPE maintains title and CDT shall have risk of loss or damage for loaner units if provided at HPE's discretion as part of hardware support or warranty services and such units will be returned to HPE without lien or encumbrance at the end of the loaner period.

Hardware Support: Compatible Cables and Connectors. CDT will connect hardware products covered under support with cables and connectors (including fiber optics if applicable) that are compatible with the system, according to the manufacturer's operating manual.

Data Backup. To reconstruct CDT lost or altered files, data, or programs, CDT must maintain a separate backup system or procedure that is not dependent on the products under support.

Temporary Workarounds. CDT will implement temporary procedures or workarounds provided by HPE while HPE works on a permanent solution after discussion with CDT as needed.

Hazardous Environment. CDT will notify HPE if CDT uses products in an environment that poses a potential health or safety hazard to HPE employees or subcontractors. HPE may require CDT to maintain such products under HPE supervision and may postpone service until CDT remedies such hazards.

Authorized Representative. CDT will have a representative present when HPE provides support at CDT site.

Product List. CDT will create, maintain and update a list of all products under support including: the location of the products, serial numbers, the HPE-designated system identifiers, and coverage levels.

Solution Center Designated Callers. CDT will identify a reasonable number of callers, as determined by HPE and CDT ("Designated Callers"), who may access HPE's CDT Support call

centers ("Solution Centers") or online help tools.

Solution Center Caller Qualifications. Designated Callers must be generally knowledgeable and demonstrate technical aptitude in system administration, system management, and, if applicable, network administration and management and diagnostic testing. HPE may review and discuss with CDT any Designated Caller's experience to determine initial eligibility. If issues arise during a call to the Solution Center that, in HPE's reasonable opinion, may be a result of a Designated Caller's lack of general experience and training, CDT may be required to replace that Designated Caller. All Designated Callers must have the proper system identifier as provided to CDT when Support is initiated. Solution Centers may provide support in English or local languages, or both.

Exhibit A, Attachment 2: Capacity Commitment

Commitment Capacity
November 1, 2020 – October 31, 2021

Support Category	Count
Dell-Remi	1
HP-Warranty	187
Blades	124
Total	312

Location	Said #	HP Reference #	Start Date	End Date
3101 GOLD CAMP DR,RANCHO CORDOVA CA	1045 5828 9161	49484783	11/01/2020	10/31/2021
3101 GOLD CAMP DR,RANCHO CORDOVA CA	1045 5828 3945	49485179	11/01/2020	10/31/2021
3101 GOLD CAMP DR,RANCHO CORDOVA CA	1045 5976 9302	49156792	11/01/2020	10/31/2021

SAID Description					
HP and HPE warranty products. Break fix support 24x7 4hr response.	1045 5828 9161	49484783	Gold Camp / Vacaville	269	1. HP - Warranty,
					2. HP D2600.D2700 - Warranty
					3. HP MSA 60.70 - REMI
					4. HP -REMI
HP and HPE warranty products. Break fix support 24x7 4hr response.	1045 5828 3945	49485179	Gold Camp / Vacaville	43	1. HP - Warranty,
					2. HP -REMI
Datacenter Care Core: Proactive deliverables and enhanced call handling. Note: Devices are currently under prepaid support for longer than the term of this DCC contract. The devices are built into this DC core SAID.	1045 5976 9302	49156792	Gold Camp / Vacaville	110	1. HPE – Warranty that does not expire during the proposed contract period.
			Total	312	

Exhibit A, Attachment 3: HPE Holidays

January 2021

- US Martin Luther King Jr. Holiday
- Company Holiday Mon Jan 18, 2021 United States

February 2021

- US President's Day Holiday
- Company Holiday Mon Feb 15, 2021 United States

May 2021

- US Memorial Day Holiday
- Company Holiday Mon May 31, 2021 United States

July 2021

- US Independence Day Holiday
- Company Holiday Sunday Jul 4, 2021 United States

September 2021

- US Labor Day Holiday
- Company Holiday Mon Sep 6, 2021 United States

November 2021

- US Thanksgiving Day Holiday
- Company Holiday Thu Nov 25, 2021 United States
- US Day following Thanksgiving Day Holiday
- Company Holiday Fri Nov 26, 2021 United States

December 2021

- US Company Designated Floating Day Holiday
- Company Holiday Sat Dec 25, 2021 United States

Exhibit A, Attachment 4: Primary / Secondary / Local Support Hub Matrix

Primary = A Primary support hub is capable of providing on-site hardware support for all HPE products and many selected non-HPE products. Examples: 24x7, 6hr CTR, 4hr Response, P24, CS.

Secondary = A Secondary support hub augments capabilities of the primary HPE Support Responsible Hub.

Local = Support contracts are not quoted out of local hubs. A local support hub augments the capabilities of primary/secondary hubs and specific CDT commitments.

Area Name	# of CEs (including GDS)	Support Hub	Address 1	Address 2	City	State	Hub Zip/Postal Code	Hub Phone #	Hub Fax #
NORTHWEST	28	CUPERTINO	19447 PRUNERIDGE AVE	M/S 4236	CUPERTINO	CA	95014	N/A	N/A
NORTHWEST	1	FRESNO			FRESNO	CA	93727	N/A	N/A
NORTHWEST	10	PLEASANTON	4430 WILLOW ROAD	SUITE 100	PLEASANTON	CA	94588	N/A	N/A
NORTHWEST	23	SACRAMENTO	300 CAPITOL MALL	SUITE 100	SACRAMENTO	CA	95834	N/A	N/A
NORTHWEST	9	SAN FRANCISCO	303 SECOND STREET	SUITE 500 SOUTH	SAN FRANCISCO	CA	94107	N/A	415-979-3708

Exhibit A, Attachment 5: Definitions

The following terms/acronyms are used throughout this SOW.

Acronym	Definition
AAT	Assigned Account Team
ADM	Account Delivery Manager
ASM	Account Support Manager
ASP	Account Support Plan
BCC	Business Critical Consultant
CEM	Critical Event Manager
CSR	CDT Self Repair
CTR	Hardware Call to Repair
CDT	California Department of Technology
DC	Datacenter Care
DM	Datacenter Care Delivery Manager
DHS	Datacenter Hardware Specialist
DMR	Defective Media Retention (optional service)
ECH	Enhanced Call Handling
HPE	Hewlett-Packard Company
HPELN	HPE Live Network
HPESC	HPE Support Center
Incident Severity	<ul style="list-style-type: none"> Severity 1 – Critical Down: for example, production environment down; production system or product application down or at severe risk; data corruption or loss or risk; business severely affected; safety issues Severity 2 – Critically Degraded: for example, production environment severely impaired; production system or production application interrupted or compromised; risk of re-occurrence; significant impact on business Severity 3 – Normal: for example, non-production or test system down or degraded; production system or production application degraded with workaround in place; non-critical functionality lost; limited impact on the business Severity 4 – Low: for example, no business or user impact
IP	Intellectual Property
ISV	Independent Software Vendor
KPI	Key Performance Indicator
LOA	Letter of Agency
LUN	Logical Unit Number
MC	Mission Critical
MCDT	Mission Critical Delivery Team – see AAT
OEM	Original Equipment Manufacturer
PM	Program Manager
PMO	Program Management Office
PSC	Proactive Service Credits
PSP	Primary Service Provider

Acronym	Definition
RCE	Response Center Engineer
SIP	Service Improvement Plan (optional service)
SLA	Service Level Agreement
SOW	Statement of Work
SPOC	Single point of Contact
Standard Work Day	Monday through Friday 8am – 5pm, local time, excluding HPE Holidays
TAM	Technical Account Manager
TC	Technical Consultant
TSS	Technical Solution Specialist
WA	Work Authorization

Exhibit A, Attachment 6: Personnel Change Order Request Form



CHANGE ORDER NO. CO-	
Contractor Name: _____ Contract Number: _____	
Proposed Start Date: _____ or upon approval by the Contract Administrator, whichever occurs later.	
<u>Reason for Change:</u> 	
<u>Description of Change:</u> To Swap out the following Personnel. Current Personnel: (Name, classification and hourly rate) Proposed Personnel: (Name including phone number and email address)	
<u>Proposed Personnel Classification:</u> (must be equal or better than current classification)	<u>Proposed Hourly Rate:</u> (must be less than or equal to current rate)
<u>Resume Attached?</u> <u>Experience Worksheet included?</u>	
<u>Approval:</u> Changes identified above are in accordance with the terms and condition of the contract. By signing below, the Contractor Official has confirmed that the proposed staff meets the personnel classification requirements and any requirements listed in the Statement of Work (SOW), Exhibit A. The Contract Administrator's signature below indicates that he/she has confirmed that the proposed personnel staff meets the requirements listed in the SOW, Exhibit A.	
Contractor Official (Print name & Sign) / Date 	CDT Contract Administrator (Print name & Sign) / Date 

Exhibit A, Attachment 7: Equipment List Template

1. SAID
2. Equipment Serial Number
3. Description of Equipment type (e.g., DL380 Gen8)
4. Location
5. Add Date
6. Add Cost
7. Remove Date
8. Remove Credit

Exhibit B: Payment and Invoicing

1. Payment/Invoicing:

- a. The initial Payment and Invoice is based on the committed purchase capacity identified in Exhibit A, Attachment 2. Subsequent Payment and Invoices are based on Monthly True-up/Review Process (Section 3). All invoices are payable monthly in arrears of service delivery period using the Equipment List template (Exhibit A, Attachment 7).
- b. Payment for Education and Training services will be made in arrears upon receipt and approval of an itemized invoice.
- c. The Contractor costs related to items such as travel and per diem are costs of the Contractor, shall be inclusive of the hourly rate bid, and will not be paid separately as part of this Contract.
- d. Payment of services will be made monthly in arrears upon receipt of a correct invoice, after delivery by the Contractor and acceptance by the State. (The Invoice Periods are defined in Section 3.) Vendor shall invoice following the Invoice Periodic for hardware maintenance services in arrears of the period for which the services are to be performed. **Invoices shall include the California Department of Technology Agreement/Agency Order Number, product name/description, part/item numbers (as applicable) and cost.**
- e. Submit CDT invoice using only **one** of the following options:
 - 1) Send via U.S. mail in **TRIPLICATE** to:

California Department of Technology
Administration Division – Accounting Office
P. O. Box 1810
Rancho Cordova, CA 95741

OR
 - 2) Submit electronically at: APIInvoices@state.ca.gov

2. Prompt Payment Act:

Payment(s) will be made in accordance with the California Prompt Payment Act, within the time specified in Government Code Chapter 4.5 commencing with Section 927.

3. Budget Act:

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

If funding for any fiscal year is reduced or deleted by the Budget Act for purposes of this program, the State shall have the option to either cancel this Contract with no liability occurring to the State, or offer a contract amendment to the Contractor to reflect the reduced amount.

EXHIBIT B-1: Capacity Equipment List Pricing by SAID

Hewlett Packard Enterprise Datacenter Care Renewal			
#	Qty.	Description	Total Price
1	1	Hewlett Packard Enterprise Datacenter Care Renewal SAID # 1045 5828 9161 Term: 11/1/20 – 10/31/21 Please reference Exhibit B-1A for Product Specifications	\$
2	1	Hewlett Packard Enterprise Datacenter Care Renewal SAID # 1045 5828 3945 Term: 11/1/20 – 10/31/21 Please reference Exhibit B-1B for Product Specifications	\$
3	1	Hewlett Packard Enterprise Datacenter Care Renewal SAID # 1045 5976 9302 Term: 11/1/20 – 10/31/21 Please reference Exhibit B-1C for Product Specifications	\$
Total			\$

Exhibit B-1A
SAID 1045 5828 9161

Support Account Reference	Service Agreement ID	From:	Coverage Period To:	Description
DCASMPD5042S1324PJ5	1045 5828 9161	11/01/2020	10/31/2021	Technology Agency Data Center

Product No.	Description	Serial No.	Coverage Period from:	to:	Qty
-------------	-------------	------------	-----------------------	-----	-----

H2T12AC

HPE Datacenter Care SVC

*** Hardware Support ***

HPE Hardware Maintenance Onsite Support

Hardware Problem Diagnosis
Onsite Support
Parts and Material provided
24 hrs, Day 6
4 Hr Onsite Response
24 hrs, Day 7
Holidays Covered
24 Hrs Std Office Days
Travel Zone 1
Defective Media Retention

686792-B21	HP DL560 Gen8 CTO Server	USE3130D6F		1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6P		1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6W		1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D77		1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D78		1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D79		1
507019-B21	HP Blc7000 CTO 3 IN LCD ROHS Encl	USE144JHWT		1
507019-B21	HP Blc7000 CTO 3 IN LCD ROHS Encl	USE144JHWW		1
507019-B21	HP Blc7000 CTO 3 IN LCD ROHS Encl	USE129CLV7		1
507019-B21	HP Blc7000 CTO 3 IN LCD ROHS Encl	USE129CLT3		1
BK766A	HP D2600 2TB 6G SAS LFF MDL 24TB Bundle	CN800401AF		1
494329-B21	HP OEM DL380G6 CTO Server	USE042N43C		1
494329-B21	HP OEM DL380G6 CTO Server	USE108N1F0		1
583914-B21	HP DL380G7 SFF CTO Server	USE131N0MR		1
583914-B21	HP DL380G7 SFF CTO Server	USE131N0MS		1
583914-B21	HP DL380G7 SFF CTO Server	USE131N0MT		1

Exhibit B-1A
SAID 1045 5828 9161

583914-B21	HP DL380G7 SFF CTO Server	USE131N0ND			1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7LM			1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7LN			1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7LP			1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7PA			1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7PG			1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7PJ			1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7PZ			1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7Q7			1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7R7			1
U1V83AS	HPE DC Environment Wide Entitlement SVC				1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270054			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005T			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427006G			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427006Q			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270079			1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	USE709AYRN			1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306LZ		01/24/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306LZ	01/25/2021		1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306M1		01/24/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306M1	01/25/2021		1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE2268ENP			1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ60508DY			1
767032-B21	HPE DL380 Gen9 24SFF CTO Server	MXQ71407XB			1
603718-B21	HP BL460c G7 CTO Blade	USE129CLT6			1
603718-B21	HP BL460c G7 CTO Blade	USE130D8MV			1
603718-B21	HP BL460c G7 CTO Blade	USE130D8MX			1
603718-B21	HP BL460c G7 CTO Blade	USE130D8N0			1
603718-B21	HP BL460c G7 CTO Blade	USE130D8N1			1
603718-B21	HP BL460c G7 CTO Blade	USE130D8N2			1
603718-B21	HP BL460c G7 CTO Blade	USE144JHXL			1
603718-B21	HP BL460c G7 CTO Blade	USE144JHYL			1
603718-B21	HP BL460c G7 CTO Blade	USE144JHYW			1
603718-B21	HP BL460c G7 CTO Blade	USE144JJ01			1
	HPE Collaborative Remote Support				
	Basic Software Phone Support				
	Collaborative Call Managemnt				
	24 Hours, Day 1-7 Phone Supp				
	Standard Response Time				
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6F			1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6P			1

Exhibit B-1A
SAID 1045 5828 9161

686792-B21	HP DL560 Gen8 CTO Server	USE3130D6W	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D77	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D78	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D79	1
507019-B21	HP BLc7000 CTO 3 IN LCD ROHS Encl	USE144JHWT	1
507019-B21	HP BLc7000 CTO 3 IN LCD ROHS Encl	USE144JHWW	1
507019-B21	HP BLc7000 CTO 3 IN LCD ROHS Encl	USE129CLV7	1
507019-B21	HP BLc7000 CTO 3 IN LCD ROHS Encl	USE129CLT3	1
494329-B21	HP OEM DL380G6 CTO Server	USE042N43C	1
494329-B21	HP OEM DL380G6 CTO Server	USE108N1F0	1
583914-B21	HP DL380G7 SFF CTO Server	USE131N0MR	1
583914-B21	HP DL380G7 SFF CTO Server	USE131N0MS	1
583914-B21	HP DL380G7 SFF CTO Server	USE131N0MT	1
583914-B21	HP DL380G7 SFF CTO Server	USE131N0ND	1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7LM	1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7LN	1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7LP	1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7PA	1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7PG	1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7PJ	1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7PZ	1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7Q7	1
583914-B21	HP DL380G7 SFF CTO Server	USE142N7R7	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270054	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005T	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427006G	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427006Q	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270079	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	USE709AYRN	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306LZ	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306M1	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE2268ENP	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ60508DY	1
767032-B21	HPE DL380 Gen9 24SFF CTO Server	MXQ71407XB	1
603718-B21	HP BL460c G7 CTO Blade	USE129CLT6	1
603718-B21	HP BL460c G7 CTO Blade	USE130D8MV	1
603718-B21	HP BL460c G7 CTO Blade	USE130D8MX	1
603718-B21	HP BL460c G7 CTO Blade	USE130D8N0	1
603718-B21	HP BL460c G7 CTO Blade	USE130D8N1	1
603718-B21	HP BL460c G7 CTO Blade	USE130D8N2	1
603718-B21	HP BL460c G7 CTO Blade	USE144JHXL	1
603718-B21	HP BL460c G7 CTO Blade	USE144JHYL	1
603718-B21	HP BL460c G7 CTO Blade	USE144JHYW	1

Exhibit B-1A
SAID 1045 5828 9161

603718-B21	HP BL460c G7 CTO Blade	USE144JJ01			1
Hardware products under warranty					
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306LZ	01/25/2018	01/24/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306M1	01/25/2018	01/24/2021	1

Exhibit B-1B
SAID 1045 5828 3945

Support Account Reference	Service Agreement ID	From:	Coverage Period To:	Description
DCASMPD504USE3204C5D	1045 5828 3945	11/01/2020	10/31/2021	Technology Agency Data Center

Product No.	Description	Serial No.	from:	Coverage Period to:	Qty
-------------	-------------	------------	-------	---------------------	-----

H2T12AC

HPE Datacenter Care SVC

*** Hardware Support ***

HPE Hardware Maintenance Onsite Support

Hardware Problem Diagnosis
Onsite Support
Parts and Material provided
24 hrs, Day 6
4 Hr Onsite Response
24 hrs, Day 7
Holidays Covered
24 Hrs Std Office Days
Travel Zone 1
Defective Media Retention

653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427004Y			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270051			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270057			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270059			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005D			1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VR3			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005L			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005P			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005Q			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005R			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005Y			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270063			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270064			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427006T			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427006V			1

Exhibit B-1B
SAID 1045 5828 3945

583914-B21	HP DL380G7 SFF CTO Server	USE2278VSC		1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427006Y		1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427006Z		1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270070		1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270073		1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VSL		1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270077		1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427007J		1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VSV		1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427007Q		1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306LZ	01/24/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306LZ	01/25/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306M1	01/24/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306M1	01/25/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003G8	06/11/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003G8	06/12/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003G9	06/11/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003G9	06/12/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GB	06/11/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GB	06/12/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GF	06/11/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GF	06/12/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GG	06/11/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GG	06/12/2021	1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VW2		1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GH	06/11/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GH	06/12/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZQ	06/16/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZQ	06/17/2021	1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VW3		1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZR	06/16/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZR	06/17/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZS	06/16/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZS	06/17/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZT	06/16/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZT	06/17/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281100VG	06/12/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281100VG	06/13/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902MH	08/11/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902MH	08/12/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902MJ	08/11/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902MJ	08/12/2021	1

Exhibit B-1B
SAID 1045 5828 3945

868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902MK		08/11/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902MK	08/12/2021		1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902ML		08/11/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902ML	08/12/2021		1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M2821020L		09/03/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M2821020L	09/04/2021		1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M282301BZ		09/03/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M282301BZ	09/04/2021		1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M282301C0		09/03/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M282301C0	09/04/2021		1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M282602XY		09/30/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M282602XY	10/01/2021		1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M282602XZ		09/30/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M282602XZ	10/01/2021		1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VWP			1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ61706XF			1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VY5			1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ61706XG			1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ61706XH			1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VYJ			1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VYM			1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VYP			1
583914-B21	HP DL380G7 SFF CTO Server	USE2278W01			1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQC		12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQC	12/26/2020		1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQD		12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQD	12/26/2020		1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQF		12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQF	12/26/2020		1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQG		12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQG	12/26/2020		1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQH		12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQH	12/26/2020		1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQJ		12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQJ	12/26/2020		1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQK		12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQK	12/26/2020		1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQL		12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQL	12/26/2020		1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE3120078			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312007C			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312007N			1

Exhibit B-1B
SAID 1045 5828 3945

653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE3120083	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE3120086	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE3120089	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312008A	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312008E	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312008F	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312008L	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312008Y	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE3120094	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE3120099	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312009A	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312009B	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312009X	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE31200A2	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE31200A4	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE31200AD	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6E	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6H	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6J	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6R	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6S	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6T	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6V	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6Y	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D70	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D71	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D72	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D74	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D75	1
686792-B21	HP DL560 Gen8 CTO Server	USE32259VE	1
686792-B21	HP DL560 Gen8 CTO Server	USE32259VR	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE3204C5S	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572M6	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572MB	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572MK	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572MR	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572MW	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572N0	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572N4	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572NA	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572ND	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572NM	1

Exhibit B-1B
SAID 1045 5828 3945

653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572NP			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572NY			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572P4			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572P6			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572PB			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572PE			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572PL			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572PM			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572PS			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572R2			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572R6			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572R8			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572RD			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572RK			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572RL			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572RX			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572RY			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572S4			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572S6			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572S7			1
U1V83AS	HPE DC Environment Wide Entitlement SVC				1
735151-B21	HP BL460c Gen8 E5-v2 10/20Gb CTO Blade	USE243K7T			1
686792-B21	HP DL560 Gen8 CTO Server	USE32259VM			1
686792-B21	HP DL560 Gen8 CTO Server	USE32259TP			1
686792-B21	HP DL560 Gen8 CTO Server	USE32259VP			1
686792-B21	HP DL560 Gen8 CTO Server	USE32259VS			1
507019-B21	HP BLc7000 CTO 3 IN LCD ROHS Encl	USE144JHWS			1
507019-B21	HP BLc7000 CTO 3 IN LCD ROHS Encl	USE144JHWV			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005G			1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005Z			1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6K			1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D73			1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D76			1
686792-B21	HP DL560 Gen8 CTO Server	USE32259V6			1
686792-B21	HP DL560 Gen8 CTO Server	USE32259V9			1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQH	01/17/2021		1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQJ	12/18/2020	12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQJ	12/26/2020		1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQC	01/17/2021		1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQG	12/18/2020	12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQG	12/26/2020		1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQL	12/18/2020	12/25/2020	1

Exhibit B-1B
SAID 1045 5828 3945

719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQL	12/26/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQK	01/17/2021	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQF	01/17/2021	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005H		1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	USE718BWVN		1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ60508LG		1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572RJ		1
455880-B21	HP Blc VC Flex-10 Enet Module Opt	3C41140016		1
455880-B21	HP Blc VC Flex-10 Enet Module Opt	3C41140017		1
455880-B21	HP Blc VC Flex-10 Enet Module Opt	3C4114001N		1
455880-B21	HP Blc VC Flex-10 Enet Module Opt	3C4114001P		1
455880-B21	HP Blc VC Flex-10 Enet Module Opt	3C413600A5		1
455880-B21	HP Blc VC Flex-10 Enet Module Opt	3C413600AG		1
455880-B21	HP Blc VC Flex-10 Enet Module Opt	3C413600N5		1
455880-B21	HP Blc VC Flex-10 Enet Module Opt	3C413600NB		1
455880-B21	HP Blc VC Flex-10 Enet Module Opt	3C413600NC		1
455880-B21	HP Blc VC Flex-10 Enet Module Opt	3C413600NF		1
455880-B21	HP Blc VC Flex-10 Enet Module Opt	3C413600NP		1
455880-B21	HP Blc VC Flex-10 Enet Module Opt	3C413600NR		1
455880-B21	HP Blc VC Flex-10 Enet Module Opt	3C423601BT		1
455880-B21	HP Blc VC Flex-10 Enet Module Opt	3C423601L3		1
572018-B21	HP Blc VC 8Gb FC 20-Port Opt Kit	6C4229Z045		1
572018-B21	HP Blc VC 8Gb FC 20-Port Opt Kit	6C4230Z00K		1
572018-B21	HP Blc VC 8Gb FC 20-Port Opt Kit	CN8114Z01C		1
572018-B21	HP Blc VC 8Gb FC 20-Port Opt Kit	CN8114Z03P		1
572018-B21	HP Blc VC 8Gb FC 20-Port Opt Kit	CN8114Z04N		1
572018-B21	HP Blc VC 8Gb FC 20-Port Opt Kit	CN8114Z0KT		1
572018-B21	HP Blc VC 8Gb FC 20-Port Opt Kit	CN8120Z02B		1
572018-B21	HP Blc VC 8Gb FC 20-Port Opt Kit	CN8120Z09Y		1
572018-B21	HP Blc VC 8Gb FC 20-Port Opt Kit	CN8120Z0EW		1
572018-B21	HP Blc VC 8Gb FC 20-Port Opt Kit	CN8120Z0HV		1
572018-B21	HP Blc VC 8Gb FC 20-Port Opt Kit	CN8120Z0NS		1
572018-B21	HP Blc VC 8Gb FC 20-Port Opt Kit	CN8123Z07S		1
572018-B21	HP Blc VC 8Gb FC 20-Port Opt Kit	CN8123Z09R		1
572018-B21	HP Blc VC 8Gb FC 20-Port Opt Kit	CN8123Z0J9		1
603718-B21	HP BL460c G7 CTO Blade	MXQ24400QT		1
603718-B21	HP BL460c G7 CTO Blade	MXQ24400QZ		1
603718-B21	HP BL460c G7 CTO Blade	MXQ24400R1		1
603718-B21	HP BL460c G7 CTO Blade	MXQ24400R3		1
603718-B21	HP BL460c G7 CTO Blade	MXQ24400R5		1
507019-B21	HP Blc7000 CTO 3 IN LCD ROHS Encl	USE243K7SC		1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7SH		1

Exhibit B-1B
SAID 1045 5828 3945

641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7VL	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7VM	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7VN	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7VR	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7VS	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7VV	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7VW	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7VX	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7VY	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W0	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W1	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W2	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W4	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W5	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W6	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W7	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W8	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W9	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WA	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WB	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WC	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WD	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WE	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WF	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WH	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WJ	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WK	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WL	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WM	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WN	1

HPE Collaborative Remote Support
Basic Software Phone Support
Collaborative Call Managemnt
24 Hours, Day 1-7 Phone Supp
Standard Response Time

653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427004Y	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270051	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270057	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270059	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005D	1

Exhibit B-1B
SAID 1045 5828 3945

583914-B21	HP DL380G7 SFF CTO Server	USE2278VR3	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005L	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005P	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005Q	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005R	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005Y	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270063	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270064	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427006T	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427006V	1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VSC	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427006Y	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427006Z	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270070	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270073	1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VSL	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M24270077	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427007J	1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VSV	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427007Q	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306LZ	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306M1	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003G8	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003G9	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GB	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GF	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GG	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GH	1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VW2	1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VW3	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZQ	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZR	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZS	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZT	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281100VG	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902MH	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902MJ	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902MK	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902ML	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M2821020L	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M282301BZ	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M282301C0	1

Exhibit B-1B
SAID 1045 5828 3945

868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M282602XY	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M282602XZ	1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VWP	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ61706XF	1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VY5	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ61706XG	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ61706XH	1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VYJ	1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VYM	1
583914-B21	HP DL380G7 SFF CTO Server	USE2278VYP	1
583914-B21	HP DL380G7 SFF CTO Server	USE2278W01	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQC	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQD	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQF	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQG	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQH	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQJ	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQK	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQL	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE3120078	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312007C	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312007N	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE3120083	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE3120086	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE3120089	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312008A	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312008E	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312008F	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312008L	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312008Y	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE3120094	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE3120099	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312009A	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312009B	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE312009X	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE31200A2	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE31200A4	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE31200AD	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6E	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6H	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6J	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6R	1

Exhibit B-1B
SAID 1045 5828 3945

686792-B21	HP DL560 Gen8 CTO Server	USE3130D6S	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6T	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6V	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6Y	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D70	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D71	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D72	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D74	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D75	1
686792-B21	HP DL560 Gen8 CTO Server	USE32259VE	1
686792-B21	HP DL560 Gen8 CTO Server	USE32259VR	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE3204C5S	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572M6	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572MB	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572MK	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572MR	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572MW	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572N0	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572N4	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572NA	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572ND	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572NM	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572NP	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572NY	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572P4	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572P6	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572PB	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572PE	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572PL	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572PM	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572PS	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572R2	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572R6	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572R8	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572RD	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572RK	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572RL	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572RX	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572RY	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572S4	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572S6	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572S7	1

Exhibit B-1B
SAID 1045 5828 3945

735151-B21	HP BL460c Gen8 E5-v2 10/20Gb CTO Blade	USE243K7T	1
686792-B21	HP DL560 Gen8 CTO Server	USE32259VM	1
686792-B21	HP DL560 Gen8 CTO Server	USE32259TP	1
686792-B21	HP DL560 Gen8 CTO Server	USE32259VP	1
686792-B21	HP DL560 Gen8 CTO Server	USE32259VS	1
507019-B21	HP BLc7000 CTO 3 IN LCD ROHS Encl	USE144JHWS	1
507019-B21	HP BLc7000 CTO 3 IN LCD ROHS Encl	USE144JHWV	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005G	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005Z	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D6K	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D73	1
686792-B21	HP DL560 Gen8 CTO Server	USE3130D76	1
686792-B21	HP DL560 Gen8 CTO Server	USE32259V6	1
686792-B21	HP DL560 Gen8 CTO Server	USE32259V9	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQH	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQJ	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQC	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQG	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQL	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQK	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQF	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	2M2427005H	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	USE718BWWN	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ60508LG	1
653200-B21	HP DL380p Gen8 8-SFF CTO Server	USE32572RJ	1
603718-B21	HP BL460c G7 CTO Blade	MXQ24400QT	1
603718-B21	HP BL460c G7 CTO Blade	MXQ24400QZ	1
603718-B21	HP BL460c G7 CTO Blade	MXQ24400R1	1
603718-B21	HP BL460c G7 CTO Blade	MXQ24400R3	1
603718-B21	HP BL460c G7 CTO Blade	MXQ24400R5	1
507019-B21	HP BLc7000 CTO 3 IN LCD ROHS Encl	USE243K7SC	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7SH	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7SJ	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7SK	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7SL	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7SM	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7SN	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7SP	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7SR	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7SS	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7ST	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7SV	1

Exhibit B-1B
SAID 1045 5828 3945

641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W1	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W2	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W4	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W5	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W6	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W7	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W8	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7W9	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WA	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WB	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WC	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WD	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WE	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WF	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WH	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WJ	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WK	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WL	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WM	1
641016-B21	HP BL460c Gen8 10/20Gb FLB CTO Blade	USE243K7WN	1

Hardware products under warranty

868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306LZ	01/25/2018	01/24/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M280306M1	01/25/2018	01/24/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003G8	06/12/2018	06/11/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003G9	06/12/2018	06/11/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GB	06/12/2018	06/11/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GF	06/12/2018	06/11/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GG	06/12/2018	06/11/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003GH	06/12/2018	06/11/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZQ	06/17/2018	06/16/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZR	06/17/2018	06/16/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZS	06/17/2018	06/16/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M281003ZT	06/17/2018	06/16/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281100VG	06/13/2018	06/12/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902MH	08/12/2018	08/11/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902MJ	08/12/2018	08/11/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902MK	08/12/2018	08/11/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M281902ML	08/12/2018	08/11/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M2821020L	09/04/2018	09/03/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M282301BZ	09/04/2018	09/03/2021	1
868704-B21	HPE DL380 Gen10 24SFF CTO Server	2M282301C0	09/04/2018	09/03/2021	1

Exhibit B-1B
SAID 1045 5828 3945

868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M282602XY	10/01/2018	09/30/2021	1
868703-B21	HPE DL380 Gen10 8SFF CTO Server	2M282602XZ	10/01/2018	09/30/2021	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQC	12/26/2017	12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQD	12/26/2017	12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQF	12/26/2017	12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQG	12/26/2017	12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQH	12/26/2017	12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQJ	12/26/2017	12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQK	12/26/2017	12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQL	12/26/2017	12/25/2020	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQH	12/26/2017	01/16/2021	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQJ	12/26/2017	12/25/2020a)	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQC	12/26/2017	01/16/2021	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQG	12/26/2017	12/25/2020a)	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQL	12/26/2017	12/25/2020a)	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQK	12/26/2017	01/16/2021	1
719064-B21	HPE DL380 Gen9 8SFF CTO Server	MXQ7500BQF	12/26/2017	01/16/2021	1

Exhibit B-1C
SAID 1045 5976 9302

Support Account Reference	Service Agreement ID	Coverage Period		Description
		From:	To:	
DCASMPD504TECHNOLOGY	1045 5976 9302	11/01/2020	10/31/2021	Technology Agency Data Center

Product No.	Description	Serial No.	Coverage Period		Qty
			from:	to:	

H2T12AC HPE Datacenter Care SVC
***** Environmental Services *****

HPE Proactive Options SVC
 Relationship Management
 Enhanced Call Handling

***** Hardware Support *****

HPE Hardware Maintenance Onsite Support
 Hardware Problem Diagnosis
 Onsite Support
 Parts and Material provided
 Svc Lvl per seprate cntrct/wty
 Cov win per seprate cntrct/wty
 Travel Zone 1

U1V83AS HPE DC Environment Wide Entitlement SVC
***** Software Support *****

1

HPE Software Technical Unlimited Support
 Cov win per seprate cntrct
 SW Technical Support
 SW Electronic Support
 Svc Lvl per seprate cntrct

HPE Software Updates SVC
HPE Recommended Doc Upd Method
License to Use & SW Updates
HPE Recommended SW Upd Method

H2T12AC

HPE Datacenter Care SVC

***** Environmental Services *****

HPE Proactive Options SVC
DatacenterCare Proactive Units

110

***** Hardware Support *****

HPE Hardware Maintenance Onsite Support
Hardware Problem Diagnosis
Onsite Support
Parts and Material provided
Svc Lvl per seprate cntrct/wty
Cov win per seprate cntrct/wty
Travel Zone 1

U1V83AS

HPE DC Environment Wide Entitlement SVC

1

***** Software Support *****

HPE Software Technical Unlimited Support
Cov win per seprate cntrct
SW Technical Support
SW Electronic Support
Svc Lvl per seprate cntrct

HPE Software Updates SVC
HPE Recommended Doc Upd Method
License to Use & SW Updates
HPE Recommended SW Upd Method

H2T12AC HPE Datacenter Care SVC

*** Environmental Services ***

HPE Proactive Options SVC

DatacenterCare Proactive Units

*** Hardware Support ***

HPE Hardware Maintenance Onsite Support

Hardware Problem Diagnosis

Onsite Support

Parts and Material provided

Svc Lvl per seprate cntrct/wty

Cov win per seprate cntrct/wty

Travel Zone 1

U1V83AS

HPE DC Environment Wide Entitlement SVC

1

*** Software Support ***

HPE Software Technical Unlimited Support

Cov win per seprate cntrct

SW Technical Support

SW Electronic Support

Svc Lvl per seprate cntrct

HPE Software Updates SVC

HPE Recommended Doc Upd Method

License to Use & SW Updates

HPE Recommended SW Upd Method

H2T12AC

HPE Datacenter Care SVC

*** Environmental Services ***

HPE Proactive Options SVC

DatacenterCare Proactive Units

*** Hardware Support ***

HPE Hardware Maintenance Onsite Support

Hardware Problem Diagnosis
Onsite Support
Parts and Material provided
Svc Lvl per seprate cntrct/wty
Cov win per seprate cntrct/wty
Travel Zone 1

U1V83AS

HPE DC Environment Wide Entitlement SVC

1

*** Software Support ***

HPE Software Technical Unlimited Support

Cov win per seprate cntrct
SW Technical Support
SW Electronic Support
Svc Lvl per seprate cntrct

HPE Software Updates SVC

HPE Recommended Doc Upd Method
License to Use & SW Updates
HPE Recommended SW Upd Method

EXHIBIT C

GENERAL PROVISIONS – INFORMATION TECHNOLOGY (GSPD-401IT – 09/05/14)

Are hereby incorporated by reference and made part of this agreement as if attached hereto. These documents can be viewed at:

Form GSPD 401, IT General Provisions, Effective 9/05/14
https://www.documents.dgs.ca.gov/dgs/fmc/gspd/pd_401IT.pdf

EXHIBIT D: Special Terms and Conditions To Safeguard 0Federal Tax Information

Federal statute, regulations and guidelines require that all contracts for services relating to the processing, storage, transmission, or reproduction of federal tax returns or return information, the programming, maintenance, repair, or testing of equipment or other property, or the providing of other services, for tax administration purposes include the provisions contained in this exhibit. (See 26 U.S.C. §6103(n); 26 C.F.R. §301.6103(n)-1(a)(2) and (d); Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies (Rev. 8-2010), Section 5.5 and Exhibit 7.)

The contractor agrees to comply with 26 U.S.C. §6103(n); 26 C.F.R. §301.6103(n)-1; IRS Publication 1075 (Rev. 8-2010); and all applicable conditions and restrictions as may be prescribed by the IRS by regulation, published rules or procedures, or written communication to the contractor. (See 26 C.F.R. §301.6103(n)-1(d); IRS Publication 1075 (Rev. 8-2010).)

I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be done under the supervision of the contractor or the contractor's employees.
- (2) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.
- (3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- (4) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
- (5) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
- (6) All computer systems receiving, processing, storing, or transmitting Federal tax information must meet the

requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.

- (7) No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.
- (8) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
- (9) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

II. CRIMINAL/CIVIL SANCTIONS

- (1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
- (2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the

sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

- (3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.
- (4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information* and Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.¹

III. INSPECTION

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

REFERENCES

26 U.S.C. §6103(n)

Pursuant to regulations prescribed by the Secretary, returns and return information may be disclosed to any person, including any person described in section 7513 (a), to the extent necessary in connection with the processing, storage, transmission, and reproduction of such returns and return information, the programming, maintenance, repair, testing, and procurement of equipment, and the providing of other

services, for purposes of tax administration.

26 C.F.R. §301.6103(n)-1 Disclosure of returns and return information in connection with procurement of property and services for tax administration purposes.

(a) *General rule.* Pursuant to the provisions of section 6103(n) of the Internal Revenue Code and subject to the requirements of paragraphs (b), (c), and (d) of this section, officers or employees of the Treasury Department, a State tax agency, the Social Security Administration, or the Department of Justice, are authorized to disclose returns and return information (as defined in section 6103(b)) to any person (including, in the case of the Treasury Department, any person described in section 7513(a)), or to an officer or employee of such person, to the extent necessary in connection with contractual procurement of—

- (1) Equipment or other property, or
- (2) Services relating to the processing, storage, transmission, or reproduction of such returns or return information, the programming, maintenance, repair, or testing of equipment or other property, or the providing of other services, for purposes of tax administration (as defined in section 6103(b)(4)).

No person, or officer or employee of such person, to whom a return or return information is disclosed by an officer or employee of the Treasury Department, the State tax agency, the Social Security Administration, or the Department of Justice, under the authority of this paragraph shall in turn disclose such return or return information for any purpose other than as described in this paragraph, and no such further disclosure for any such described purpose shall be made by such person, officer, or employee to anyone, other than another officer or employee of such person whose duties or responsibilities require such disclosure for a purpose described in this paragraph, without written approval by the Internal Revenue Service.

(b) *Limitations.* For purposes of paragraph (a) of this section, disclosure of returns or return information in connection with contractual procurement of property or services described in such paragraph will be treated as necessary only if such procurement or the performance of such services cannot otherwise be reasonably, properly, or economically carried out or performed without such disclosure.

Thus, for example, disclosures of returns or return information to employees of a contractor for purposes of programming, maintaining, repairing, or testing computer equipment used by the Internal Revenue Service or a State tax agency should be made only if such services cannot be reasonably, properly, or economically performed by use of information or other data in a form which does not identify a particular taxpayer. If, however, disclosure of returns or return information is in fact necessary in order for such employees to reasonably, properly, or economically perform the computer related services, such disclosures should be restricted to returns or return information selected or appearing at random. Further,

¹ A 30 minute disclosure awareness training video produced by the IRS can be found at

<http://www.irsvideos.gov/Governments/Safeguards/DisclosureAwarenessTrainingPub4711>

for purposes of paragraph (a), disclosure of returns or return information in connection with the contractual procurement of property or services described in such paragraph should be made only to the extent necessary to reasonably, properly, or economically conduct such procurement activity. Thus, for example, if an activity described in paragraph (a) can be reasonably, properly, and economically conducted by disclosure of only parts or portions of a return or if deletion of taxpayer identity information (as defined in section 6103(b)(6) of the Code) reflected on a return would not seriously impair the ability of the contractor or his officers or employees to conduct the activity, then only such parts or portions of the return, or only the return with taxpayer identity information deleted, should be disclosed.

(c) *Notification requirements.* Persons to whom returns or return information is or may be disclosed as authorized by paragraph (a) of this section shall provide written notice to their officers or employees—

- (1) That returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized by paragraph (a) of this section;
- (2) That further inspection of any returns or return information for a purpose or to an extent unauthorized by paragraph (a) of this section constitutes a misdemeanor, punishable upon conviction by a fine of as much as \$1,000, or imprisonment for as long as 1 year, or both, together with costs of prosecution;
- (3) That further disclosure of any returns or return information for a purpose or to an extent unauthorized by paragraph (a) of this section constitutes a felony, punishable upon conviction by a fine of as much as \$5,000, or imprisonment for as long as 5 years, or both, together with the costs of prosecution;
- (4) That any such unauthorized further inspection or disclosure of returns or return information may also result in an award of civil damages against any person who is not an officer or employee of the United States in an amount not less than \$1,000 for each act of unauthorized inspection or disclosure or the sum of actual damages sustained by the plaintiff as a result of such unauthorized disclosure or inspection as well as an award of costs and reasonable attorneys fees; and
- (5) If such person is an officer or employee of the United States, a conviction for an offense referenced in paragraph (c)(2) or (c)(3) of this section shall result in dismissal from office or discharge from employment.

(d) *Safeguards.* Any person to whom a return or return information is disclosed as authorized by paragraph (a) of this section shall comply with all applicable conditions and requirements which may be prescribed by the Internal Revenue Service for the purposes of protecting the confidentiality of returns and return information and preventing disclosures of returns or return information in a manner unauthorized by paragraph (a). The terms of any contract between the Treasury Department, a State

tax agency, the Social Security Administration, or the Department of Justice, and a person pursuant to which a return or return information is or may be disclosed for a purpose described in paragraph (a) shall provide, or shall be amended to provide, that such person, and officers and employees of the person, shall comply with all such applicable conditions and restrictions as may be prescribed by the Service by regulation, published rules or procedures, or written communication to such person. If the Service determines that any person, or an officer or employee of any such person, to whom returns or return information has been disclosed as provided in paragraph (a) has failed to, or does not, satisfy such prescribed conditions or requirements, the Service may take such actions as are deemed necessary to ensure that such conditions or requirements are or will be satisfied, including—

- (1) Suspension or termination of any duty or obligation arising under a contract with the Treasury Department referred to in this paragraph or suspension of disclosures by the Treasury Department otherwise authorized by paragraph (a) of this section, or
- (2) Suspension of further disclosures of returns or return information by the Service to the State tax agency, or to the Department of Justice, until the Service determines that such conditions and requirements have been or will be satisfied.

(e) *Definitions.* For purposes of this section—

- (1) The term *Treasury Department* includes the Internal Revenue Service and the Office of the Chief Counsel for the Internal Revenue Service;
- (2) The term *State tax agency* means an agency, body, or commission described in section 6103(d) of the Code; and
- (3) The term *Department of Justice* includes offices of the United States Attorneys.

IRS Publication 1075 (Rev. 8-2010) Section 5.5 Control over Processing

Processing of FTI, in an electronic media format, including removable media, microfilms, photo impressions, or other formats (including tape reformatting or reproduction or conversion to punch cards, digital images or hard copy printout) will be performed pursuant to one of the following procedures:

5.5.1 Agency Owned and Operated Facility

Processing under this method will take place in a manner that will protect the confidentiality of the information on the electronic media. All safeguards outlined in this publication also must be followed and will be subject to IRS safeguard reviews.

5.5.2 Contractor or Agency Shared Facility – Consolidated Data Centers

Recipients of FTI are allowed to use a shared facility but only in a manner that does not allow access to FTI by employees,

agents, representatives or contractors of other agencies using the shared facility.

Note: For purposes of applying sections 6103(l), (m) and (n), the term "agent" includes contractors. Access restrictions pursuant to the IRC authority by which the FTI is received continue to apply. For example, since human services agencies administering benefit eligibility programs may not allow contractor access to any FTI received, their data within the consolidated data center may not be accessed by any contractor of the data center.

The requirements in Exhibit 7, Contract Language for General Services, must be included in the contract in accordance with IRC Section 6103(n).

The contractor or agency-shared computer facility is also subject to IRS safeguard reviews.

Note: The above rules also apply to releasing electronic media to a private contractor or other agency office even if the purpose is merely to erase the old media for reuse.

Agencies utilizing consolidated data centers must implement appropriate controls to ensure the protection of FTI, including a service level agreement (SLA) between the agency authorized to receive FTI and the consolidated data center. The SLA should cover the following:

1. The consolidated data center is considered to be a "contractor" of the agency receiving FTI. The agency receiving FTI – whether it is a state revenue, workforce, child support enforcement or human services agency – is responsible for ensuring the protection of all FTI received. However, as the "contractor" for the agency receiving FTI, the consolidated data center shares responsibility for safeguarding FTI as well.
2. Provide written notification to the consolidated data center management that they are bound by the provisions of Publication 1075, relative to protecting all federal tax information within their possession or control. The SLA should also include details concerning the consolidated data center's responsibilities during a safeguard review and support required to resolve identified findings.
3. The agency will conduct an internal inspection of the consolidated data center every eighteen months (see section 6.3). Multiple agencies sharing a consolidated data center may partner together to conduct a single, comprehensive internal inspection. However, care should be taken to ensure agency representatives do not gain unauthorized access to other agency's FTI during the internal inspection.
4. The employees from the consolidated data center with access to FTI, including system administrators and programmers, must receive disclosure awareness training prior to access to FTI and annually thereafter and sign a confidentiality statement. This provision also extends to any contractors hired by the

consolidated data center that has access to FTI.

5. The specific data breach incident reporting procedures for all consolidated data center employees and contractors. The required disclosure awareness training must include a review of these procedures.
6. The Exhibit 7 language must be included in the contract between the recipient agency and the consolidated data center, including all contracts involving contractors hired by the consolidated data center.
7. Identify responsibilities for coordination of the 45-day notification of the use of contractors or sub-contractors with access to FTI.

Note: Generally, consolidated data centers are either operated by a separate state agency (example: Department of Information Services) or by a private contractor. If an agency is considering transitioning to either a state owned or private vendor consolidated data center, the Office of Safeguards strongly suggests the agency submit a request for discussions with Safeguards as early as possible in the decision-making or implementation planning process. The purpose of these discussions is to ensure the agency remains in compliance with safeguarding requirements during the transition to the consolidated data center.

26 U.S.C. §7213. Unauthorized disclosure of information

(a) Returns and return information

(1) Federal employees and other persons

It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information (as defined in section 6103(b)). Any violation of this paragraph shall be a felony punishable upon conviction by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

(2) State and other employees

It shall be unlawful for any person (not described in paragraph (1)) willfully to disclose to any person, except as authorized in this title, any return or return information (as defined in section 6103(b)) acquired by him or another person under subsection (d), (i)(3)(B)(i) or (7)(A)(ii), (l)(6), (7), (8), (9), (10), (12), (15), (16), (19), or (20) or (m)(2), (4), (5), (6), or (7) of section 6103.

Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(3) Other persons

It shall be unlawful for any person to whom any return or return information (as defined in section 6103(b)) is disclosed in a manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(4) Solicitation

It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information (as defined in section 6103(b)) and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(5) Shareholders

It shall be unlawful for any person to whom a return or return information (as defined in section 6103(b)) is disclosed pursuant to the provisions of section 6103(e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law. Any violation of this paragraph shall be a felony punishable by a fine in any amount not to exceed \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(b) Disclosure of operations of manufacturer or producer

Any officer or employee of the United States who divulges or makes known in any manner whatever not provided by law to any person the operations, style of work, or apparatus of any manufacturer or producer visited by him in the discharge of his official duties shall be guilty of a misdemeanor and, upon conviction thereof, shall be fined not more than \$1,000, or imprisoned not more than 1 year, or both, together with the costs of prosecution; and the offender shall be dismissed from office or discharged from employment.

(c) Disclosures by certain delegates of Secretary

All provisions of law relating to the disclosure of information, and all provisions of law relating to penalties for unauthorized disclosure of information, which are applicable in respect of any function under this title when performed by an officer or employee of the Treasury Department are likewise applicable in respect of such function when performed by any person who is a "delegate" within the meaning of section 7701(a)(12)(B).

(d) Disclosure of software

Any person who willfully divulges or makes known software (as defined in section 7612(d)(1)) to any person in violation of section 7612 shall be guilty of a felony and, upon conviction thereof, shall be fined not more than \$5,000, or imprisoned not more than 5 years, or both, together with the costs of prosecution.

(e) Cross references

(1) Penalties for disclosure of information by preparers of returns

For penalty for disclosure or use of information by preparers of returns, see section 7216.

(2) Penalties for disclosure of confidential information

For penalties for disclosure of confidential information by any officer or employee of the United States or any department or agency thereof, see 18 U.S.C. 1905.

26 U.S.C. §7213A. Unauthorized inspection of returns or return information

(a) Prohibitions

(1) Federal employees and other persons
It shall be unlawful for—

(A) any officer or employee of the United States, or

(B) any person described in subsection (l)(18) or (n) of section 6103 or an officer or employee of any such person, willfully to inspect, except as authorized in this title, any return or return information.

(2) State and other employees

It shall be unlawful for any person (not described in paragraph (1)) willfully to inspect, except as authorized in this title, any return or return information acquired by such person or another person under a provision of section 6103 referred to in section 7213 (a)(2) or under section 6104 (c).

(b) Penalty

(1) In general

Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding \$1,000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

(2) Federal officers or employees

An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.

(c) Definitions

For purposes of this section, the terms "inspect", "return", and "return information" have the respective meanings given such terms by section 6103 (b).

26 U.S.C. §7431. Civil damages for unauthorized inspection or disclosure of returns and return information

(a) In general

(1) Inspection or disclosure by employee of United States

If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.

(2) Inspection or disclosure by a person who is not an employee of United States

If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section [6103](#), such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(b) Exceptions

No liability shall arise under this section with respect to any inspection or disclosure -

- (1) which results from a good faith, but erroneous, interpretation of section [6103](#), or
- (2) which is requested by the taxpayer.

(c) Damages

In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of -

(1) the greater of -

(A) \$1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

(B) the sum of -

(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus

(ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) the costs of the action, plus

(3) in the case of a plaintiff which is described in section [7430\(c\)\(4\)\(A\)\(ii\)](#), reasonable attorneys fees, except that if the defendant is the United States, reasonable attorneys fees may be awarded only if the plaintiff is the prevailing party (as determined under section [7430\(c\)\(4\)](#)).

(d) Period for bringing action

Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

(e) Notification of unlawful inspection and disclosure

If any person is criminally charged by indictment or information with inspection or disclosure of a taxpayer's return or return information in violation of -

- (1) paragraph (1) or (2) of section [7213\(a\)](#),
- (2) section [7213A\(a\)](#), or
- (3) subparagraph (B) of section 1030(a)(2) of title 18, United States Code, the Secretary shall notify such

taxpayer as soon as practicable of such inspection or disclosure.

(f) Definitions

For purposes of this section, the terms "inspect", "inspection", "return", and "return information" have the respective meanings given such terms by section [6103\(b\)](#).

(g) Extension to information obtained under section [3406](#)

For purposes of this section -

(1) any information obtained under section [3406](#) (including information with respect to any payee certification failure under subsection (d) thereof) shall be treated as return information, and

(2) any inspection or use of such information other than for purposes of meeting any requirement under section [3406](#) or (subject to the safeguards set forth in section [6103](#)) for purposes permitted under section [6103](#) shall be treated as a violation of section [6103](#). For purposes of subsection (b), the reference to section [6103](#) shall be treated as including a reference to section [3406](#).

(h) Special rule for information obtained under section [6103\(k\)\(9\)](#)

For purposes of this section, any reference to section [6103](#) shall be treated as including a reference to section [6311\(e\)](#).

EXHIBIT E SECURITY AND DATA PROTECTION

Contractor shall certify to the State compliance with applicable industry standards and guidelines, including but not limited to relevant security provisions of the California State Administrative Manual (SAM), California Statewide Information Management Manual (SIMM), The National Institute of Standards and Technology (NIST) 800-53 v4 and Federal Information Processing Standard (FIPS) Publication 199 which protect and minimize risk to the State. At a minimum, provision shall cover the following:

1. The Contractor assumes responsibility of the confidentiality, integrity and availability of the data under its control. The Contractor shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards at all times during the term of the Agreement to secure such data from data breach or loss, protect the data and information assets from breaches, introduction of viruses, disabling of devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its data or affects the integrity of that data.
2. Confidential, sensitive or personal information shall be encrypted in accordance with SAM 5350.1 and SIMM 5305-A.
3. The Contractor shall comply with statewide policies and laws regarding the use and protection of information assets and data. Unauthorized use of data by Contractor or third parties is prohibited.
4. Signed Security and Confidentiality Statement for all personnel assigned during the term of the Agreement.
5. Apply security patches and upgrades, and keep virus protection software up-to-date on all information asset on which data may be stored, processed, or transmitted.
6. The Contractor shall notify the State data owner immediately if a security incident involving the information asset occurs.
7. The State data owner shall have the right to participate in the investigation of a security incident involving its data or conduct its own independent investigation. The Contractor shall allow the State reasonable access to security logs, latency statistics, and other related security data that affects this Agreement and the State's data, at no cost to the State.
8. The Contractor shall be responsible for all costs incurred by the State due to security incident resulting from the Contractor's failure to perform or negligent acts of its personnel, and resulting in an unauthorized disclosure, release, access, review, destruction; loss, theft or misuse of an information asset. If the contractor experiences a loss or breach of data, the contractor shall immediately report the loss or breach to the State. If the State data owner determines that notice to the individuals whose data has been lost or breached is appropriate, the contractor will bear any and all costs associated with the notice or any mitigation selected by the data owner. These costs include, but are not limited to, staff time, material costs, postage, media announcements, and other identifiable costs associated with the breach or loss of data.
9. The Contractor shall immediately notify and work cooperatively with the State data owner to respond timely and correctly to public records act requests.
10. The Contractor will dispose of records of State data as instructed by the State during the term of this agreement. No data shall be copied, modified, destroyed or deleted by the Contractor other than for normal operation or maintenance during the Agreement period without prior written notice to and written approval by the State.
11. Remote access to data from outside the territorial United States, including remote access to data by authorized support staff in identified support centers, is prohibited unless approved in advance by the State.
12. The physical location of Contractor's data center where the Data is stored shall be within the territorial United States.

**ATTACHMENT 1
REQUIREMENTS CHECKLIST**

Please complete the required Requirements Checklists to confirm that all items are contained with your RFQ response. Place a check mark or “✓” next to each item that you are submitting to the State.

1. Administrative Checklist

Check ✓	Attachment #	Name/Description	Form Provided	Required
	Section I.7.C	Cover Letter	NO	YES
	Attachment 1	Administrative Requirements Checklist	YES	YES
	Attachment 2	Confidentiality Statement	YES	YES
	Attachment 3	Payee Data Record, STD 204	YES	YES
	Attachment 4	Certification with the Secretary of State	LINK	YES
	Attachment 5	California Civil Rights Laws Certification	YES	YES
	Attachment 6	Pre-Employment Criminal Background Check	YES	UPON AWARD
	Attachment 7	Bidder Declaration	YES	YES
	Attachment 8	Commercially Useful Function Certification	YES	YES
	Attachment 9	Bidder Agreement to Technical Requirements	YES	YES
	EXHIBITS	EXHIBIT NAME/DESCRIPTION		
	Exhibit B-1	Cost Worksheet	YES	YES
	OTHER	DESCRIPTION		
	Final RFQ Response	One (1) Master Copy of IFB Bid and one (1) additional copies	N/A	YES
	Electronic Copy of RFQBid	One (1) Electronic Copy of IFB Bid on CD or Flash Drive	N/A	YES
	OPTIONAL	DESCRIPTION		
	Section V.10	TACPA Preferences	LINK	OPTIONAL

2. Technical Requirements Checklist

Check ✓	Mandatory Requirements	Reference in Vendor's Response (cite section and page number)
	Bidder must possess at least five (5) years' experience, reselling HPE professional services, which will be verified during evaluation.	
	Bidder must be an authorized HPE reseller, which will be verified during evaluations.	
	Bidder must be authorized to provide Datacenter Care Service Support Level, which will be verified during evaluations.	
	Bidder must possess all licenses and certifications necessary to perform the services described in Exhibit A, SOW. This includes but is not limited to approved Secretary of State certification and California Business License, sellers permit. The State will review all certificates prior to awarding contract.	

ATTACHMENT 2
CONFIDENTIALITY STATEMENT

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

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

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

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

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

All personnel assigned to this Project shall be provided a confidentiality and non-disclosure statement and will be expected to sign and return it to the representative listed below before beginning work on this project.

Signature of representative Title Date

Typed name of representative

Typed title of representative

Typed name of company

ATTACHMENT 3
PAYEE DATA RECORD (STD. 204)

Refer to the following website link to obtain the appropriate form.

<http://www.documents.dgs.ca.gov/dgs/fmc/pdf/std204.pdf>

ATTACHMENT 4
CERTIFICATION WITH THE SECRETARY OF STATE

If required by law, the Prime Contractor must provide certification through the California Secretary of State (SOS) to do business in the State of California. If the Bidder does not currently have this certification, the firm must be certified before a Contract award can be made, and must provide information in the Final Bid to support the status of its application to be certified to do business in the State of California.

Domestic and foreign Corporations, Limited Liability Companies (LLCs), Limited Liability Partnerships (LLPs) and Limited Partnerships (LPs) must be registered with the California SOS to be awarded the Contract. The SOS Certificate of Status must be included with the bid. The required document(s) may be obtained through the SOS, Certification and Records Unit at (916) 657-5448 or through the following website: <https://businesssearch.sos.ca.gov/>

**ATTACHMENT 5
 CALIFORNIA CIVIL RIGHTS LAWS CERTIFICATION**

Pursuant to Public Contract Code section 2010, if a bidder or proposer executes or renews a contract over \$100,000 on or after January 1, 2017, the bidder or proposer hereby certifies compliance with the following:

1. CALIFORNIA CIVIL RIGHTS LAWS: For contracts over \$100,000 executed or renewed after January 1, 2017, the contractor certifies compliance with the Unruh Civil Rights Act (Section 51 of the Civil Code) and the Fair Employment and Housing Act (Section 12960 of the Government Code); and

2. EMPLOYER DISCRIMINATORY POLICIES: For contracts over \$100,000 executed or renewed after January 1, 2017, if a Contractor has an internal policy against a sovereign nation or peoples recognized by the United States government, the Contractor certifies that such policies are not used in violation of the Unruh Civil Rights Act (Section 51 of the Civil Code) or the Fair Employment and Housing Act (Section 12960 of the Government Code).

CERTIFICATION

I, the official named below, certify under penalty of perjury under the laws of the State of California that the foregoing is true and correct. <i>Proposer/Bidder Firm Name (Printed)</i>	<i>Federal ID Number</i>
<i>By (Authorized Signature)</i>	
<i>Printed Name and Title of Person Signing</i>	
<i>Date Executed</i>	<i>Executed in the County and State of</i>

ATTACHMENT 6
PRE-EMPLOYMENT CRIMINAL BACKGROUND INVESTIGATION
POLICY CERTIFICATION

All contractor¹ responsibilities described below must be met prior to the commencement of the deliverables prescribed in the contract.

1. Ensuring the background check clearance of all employees designated under the prospective contract that may have access to confidential and sensitive information and data on the network or computing infrastructure;
2. Reviewing the background information and determining the employee poses no threat to the public interest or the integrity or effectiveness of the Department of Technology's mission and business;
3. Should an employee fail the background check, the Contractor will have an opportunity to replace the designated employee under the contract within 5 working days if contract work has not commenced. If the Contractor does not have another employee to fulfill the engagement, the contract will not be award and another contractor will be selected (2nd bidder);
4. All costs associated with the background check;
5. Provide certification that the vendor has met the requirements of G.C. 11546.6; and
6. For the duration of the contract, ensure the status of the employee's criminal history has not changed. If at any time, the employee does not meet the requirements of employment (see Department of Technology's Background Check policy), the Contractor is responsible for immediately notifying Department of Technology and replacing the employee. If another employee is not available, the contract shall be terminated for cause.

All contractors shall be subject to audit to ensure compliance with the special terms and conditions as described above and any related policies. Failure to comply with these terms and conditions shall constitute breach of contract and may result in contract termination for cause and penalties of \$10,000 per day for each day the Contractor was out of compliance. Contractors agree to make available for audit all background check documentation within 24 hours of notice. The CDT retains the rights to conduct its own background check at a later time, if deemed necessary.

REPRESENTATIVE NAME	TITLE	PHONE NUMBER
COMPANY NAME		
STREET ADDRESS		
CITY	STATE	ZIP CODE

SIGNATURE

DATE

¹ For purposes of this bulletin and any related special terms and conditions, contractor means any company, organization, group or individual doing work for the Department of Technology or at any Department of Technology facility, whether they are the contract holder, the holder of a subcontract or working as a consultant.

ATTACHMENT 7
BIDDER DECLARATION

All Contractors must complete the Bidder Declaration GSPD-05-105 and include it with the bid response.

<http://www.documents.dgs.ca.gov/pd/delegations/GSPD105.pdf>

ATTACHMENT 8
COMMERCIALLY USEFUL FUNCTION CERTIFICATION

Date: _____

Name of Bidder: _____

A business that is performing a commercially useful function is one that does all of the following:

- 1) Is responsible for the execution of a distinct element of the work of the Contract.
- 2) Carries out its obligation by actually performing, managing or supervising the work involved.
- 3) Performs work that is normal for its business, services and function.
- 4) Is responsible, with respect to products, inventories, materials, and supplies required for the contract, for negotiating price, determining quality and quantity, ordering, installing, if applicable, and making payment.
- 5) Is not further subcontracting a portion of the work that is greater than that expected to be subcontracted by normal industry practices.

The Bidder must provide a written statement below detailing the role, services and/or goods the Subcontractor(s) will provide to meet the Commercially Useful Function requirement.

ATTACHMENT 9
BIDDER AGREEMENT TO ALL REQUIREMENTS OF RFQ 20-0029458, EXHIBIT A,
STATEMENT OF WORK and EXHIBIT B, PAYMENT AND INVOICING

Name: _____

Title: _____

Signature: _____

Company Name: _____

Date: _____