

SECTION A - SOLICITATION/CONTRACT FORM

A.1 EXECUTIVE SUMMARY

1. Acquisition Strategy Information

This Contract is awarded using North American Industry Classification Systems (NAICS) Code 541519 (Other Computer Related Services), Information Technology (IT) Value Added Reseller (VAR) exception, Footnote 18, for which the small business size standard is 150 employees. All awardees must comply with the Limitations on Subcontracting as outlined in Federal Acquisition Regulation (FAR) clause 52.219-14.

2. Type of Contract

This is an Indefinite-Delivery Indefinite-Quantity (IDIQ) contract awarded under FAR Part 15 (Contracting by Negotiation). Firm-Fixed Price (FFP) and/or Time and Materials (T&M) Delivery Orders (DOs) shall be competed and issued therefrom, unless an exception to fair opportunity is otherwise justified. FFP and T&M requirements are identified in the applicable contract line items in Section B of this Contract.

3. Contract Term

The term of this Commodities Enterprise Contract (CEC) is five (5) years. There are five (5), twelve (12)-month ordering periods for which pricing has been established. DOs may be issued at any time during the five (5)-year contract term utilizing the procedures at FAR Subpart 16.505 regarding fair opportunity, or exceptions thereto, for multiple award IDIQ contracts. Individual DOs may include options for Standard Extended Warranties and/or Premium Extended Warranties. In such instances, performance of the applicable DO(s) awarded prior to contract expiration may require continued warranty and technical support services, as described in Section 9.0 of the Performance Work Statement, beyond the five (5)-year contract term. FAR Clauses 52.217-7, Option for Increased Quantity – Separately Priced Line Item and 52.217-9, Option to Extend the Term of the Contract, are incorporated in this contract for incorporation into future DOs as appropriate.

4. Additional Ordering Information

The following Sub Line Item Numbers (SLINs), and as set forth in Schedule B, are “contract specific” and will be ordered on a one-time basis with the first DO issued under this Contract. The performance period for the first DO will be sixty (60) months to capture the basic contract program management requirements and delivery of “contract specific” SLINS.

SLIN 0026AA - Post Award Conference Meeting Minutes
SLIN 0026AB - Action Item Summary (Contract Post Award Conference)
SLIN 0026AC - Initial Draft Contract Level Work Plan and Schedule
SLIN 0026AD - Program Review Minutes
SLIN 0026AE - Action Item Summary (Program Reviews)

SLIN 0026AF – Updated Contract Level Work Plan and Schedule
SLIN 0026AJ - CEC Ordering Portal Information and Updates
SLIN 0026AK – Catalog
SLIN 0026AL – Change Management Plan
SLIN 0026AM – Technology Refresh Engineering Change Proposal
SLIN 0026AN – Technology Insertion Engineering Change Proposal

Engineering Change Proposals (ECPs) for SLINs 0026AM and 0026AN shall be submitted, as required, based upon the applicable requirements for Technology Refresh and Technology Insertion as specified in the CEC PWS, set forth in Section C.

The following SLINs are “DO specific” requirements and will be ordered on each applicable DO:

SLIN 0026AG – Project Management Plan and Updates
SLIN 0026AH – Monthly Progress Reports

5. Option Information

There are no options associated with the basic contract, however, the requirements for Standard Extended Warranty and Premium Extended Warranty may be included in a DO as options. To address these instances, FAR 52.217-7 Option for Increased Quantity – Separately Priced Line Item and FAR 52.217-9, Option to Extend the Term of the Contract, are included in the basic contract for applicability to individual Delivery Orders, as appropriate.

6. Performance Work Statement Attachments

All PWS Attachments are provided as attachments in Section J.

7. Maximum CEC Program Value

In accordance with Section I, FAR clause 52.216-22 entitled, “Indefinite Quantity,” the maximum value of the CEC Program is \$5,314,335,810.00. Accordingly, the cumulative value of all FFP and T&M Task Orders issued under the CEC Program shall not exceed \$5,314,335,810.00.

8. Pricing Attachment

In accordance with the Solicitation the Contractor’s Price List for IT Hardware Commodity Products, Standard Extended Warranty, Premium Extended Warranty, and Standard Installation FFP items submitted as Price.pdf as part of its Price offer has become the Offeror’s Price List for FFP items under this Contract and has been incorporated as Attachment No. 009. Prices for all FFP items listed in the Offeror’s Price List reflect the Government’s maximum price liability for the applicable item regardless of quantity ordered under subsequent DOs.

9. Government Furnished Property (GFP)

To address GFP requirements associated with individual DOs, FAR 52.245-1, Government Property, and FAR 52.245-9, Use and Charges, are incorporated into this contract.

A.2 GOVERNING LAW

Federal law and regulations, including the Federal Acquisition Regulations (“FAR”), shall govern this Contract. Commercial license agreements may be made a part of this Contract but only if both parties expressly make them an addendum. If the commercial license agreement is not made an addendum, it shall not apply, govern, be a part of or have any effect whatsoever on the Contract; this includes, but is not limited to, any agreement embedded in the computer software (clickwrap) or any agreement that is otherwise delivered with or provided to the Government with the commercial computer software or documentation (shrinkwrap), or any other license agreement otherwise referred to in any document. If a commercial license agreement is made an addendum, only those provisions addressing data rights regarding the Government’s use, duplication and disclosure of data (e.g., restricted computer software) are included and made a part of this Contract, and only to the extent that those provisions are not duplicative or inconsistent with Federal law, Federal regulation, the incorporated FAR clauses and the provisions of this Contract; those provisions in the commercial license agreement that do not address data rights regarding the Government’s use, duplication and disclosure of data shall not be included or made a part of the Contract. Federal law and regulation, including without limitation, the Contract Disputes Act (41 U.S.C. §601-613), the Anti-Deficiency Act (31 U.S.C. §1341, et seq.), the Competition in Contracting Act (41 U.S.C. §253), the Prompt Payment Act (31 U.S.C. §3901, et seq.) and FAR clauses 52.212-4, 52.227-14, 52.227-19 shall supersede, control and render ineffective any inconsistent, conflicting or duplicative provision in any commercial license agreement. In the event of conflict between this clause and any provision in the Contract or the commercial license agreement or elsewhere, the terms of this clause shall prevail. Claims of patent or copyright infringement brought against the Government as a party shall be defended by the U.S. Department of Justice (DOJ). 28 U.S.C. § 516. At the discretion of DOJ, the Contractor may be allowed reasonable participation in the defense of the litigation. Any additional changes to the Contract must be made by order modification (Standard Form 30). Nothing in this Contract or any commercial license agreement shall be construed as a waiver of sovereign immunity.

Table of Contents

PART I - THE SCHEDULE	1
SECTION A - SOLICITATION/CONTRACT FORM.....	1
SF 26 – AWARD/CONTRACT	1
A.1 EXECUTIVE SUMMARY.....	2
A.2 GOVERNING LAW.....	5
SECTION B - SUPPLIES OR SERVICES AND PRICE/COSTS	8
B.1 PRICE SCHEDULE.....	8
SECTION C - DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK.....	23
C.1 PERFORMANCE WORK STATEMENT.....	23
SECTION D - PACKAGING AND MARKING.....	65
D.1 PACKAGING, HANDLING, STORAGE AND TRANSPORTATION.....	65
SECTION E - INSPECTION AND ACCEPTANCE.....	66
E.1 52.246-2 INSPECTION OF SUPPLIES-FIXED-PRICE (AUG 1996)	66
E.2 52.246-4 INSPECTION OF SERVICES-FIXED PRICE (AUG 1996).....	66
E.3 52.246-6 INSPECTION –TIME-AND-MATERIAL AND LABOR-HOUR (MAY 2001).....	66
E.4 52.246-16 RESPONSIBILITY FOR SUPPLIES (APR 1984)	66
E.5 VAAR 852.246-71 INSPECTION (JAN 2008).....	66
E.6 VAAR 852.246-70 GUARANTEE (JAN 2008).....	66
SECTION F - DELIVERIES OR PERFORMANCE.....	67
F.1 52.242-15 STOP-WORK ORDER (AUG 1989).....	67
F.2 52.242-17 GOVERNMENT DELAY OF WORK (APR 1984).....	67
F.3 52.247-34 F.O.B. DESTINATION (NOV 1991).....	67
SECTION G - CONTRACT ADMINISTRATION DATA.....	68
G.1 CONTRACT ADMINISTRATION RESPONSIBILITIES.....	68
G.2 DELIVERY ORDER SOLICITATION.....	68
G.3 DELIVERY ORDER PROCEDURES.....	68
G.4 DELIVERY ORDER CONTENTS AND ISSUANCE.....	69
G.5 FAIR OPPORTUNITY.....	70
G.6 INVOICING AND PAYMENT.....	70
G.7 LIMITATIONS ON SUBCONTRACTING – MONITORING AND COMPLIANCE.....	70
SECTION H - SPECIAL CONTRACT REQUIREMENTS.....	71
H.1 TERM OF CONTRACT.....	71
H.2 CONTRACT TOTAL MINIMUM AD MAXIMUM QUANTITIES.....	71
H.3 AGENCY DELIVERY ORDER OMBUDSMAN.....	71
H.4 ACTIVITIES AUTHORIZED TO ISSUE ORDERS.....	71
H.5 CEC IT HARDWARE COMMODITY CEILING PRICES	72
H.6 CEC INCIDENTAL TECHNICAL SUPPORT SERVICES CEILING PRICE.....	72
H.7 ORDERING PERIODS.....	72
H.8 ON-RAMP/OFF-RAMP.....	72

PART II - CONTRACT CLAUSES.....	74
SECTION I - CONTRACT CLAUSES.....	74
I.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998).....	74
I.2 52.209-9 UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS (JAN 2011)	77
I.3 52.216-18 ORDERING (OCT 1995).....	77
I.4 52.216-19 ORDER LIMITATIONS (OCT 1995).....	77
I.5 52.216-22 INDEFINITE QUANTITY (OCT 1995).....	78
I.6 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000).....	78
I.7 52.219-28 POST-AWARD SMALL BUSINESS PROGRAM REPRESENTATION (APR 2009)...	79
I.8 52.222-40 NOTIFICATION OF EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT (DEC 2010).....	80
I.9 52.227-3 PATENT INDEMNITY (APR 1984).....	81
I.10 52.246-20 WARRANTY OF SERVICES (MAY 2001).....	82
I.11 VAAR 852.211-75 PRODUCT SPECIFICATIONS (JAN 2008)	82
I.12 VAAR 852.215-71 EVALUATION FACTOR COMMITMENTS (DEC 2009)	83
I.13 VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984)	83
I.14 VAAR 852.270-1 REPRESENTATIVES OF CONTRACTING OFFICERS (JAN 2008).....	83
I.15 VAAR 852.273-75 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (Interim - October 2008).....	83
I.16 VAAR 852.273-76 ELECTRONIC INVOICE SUBMISSION (Interim - October 2008).....	84
I.17 SUPPLEMENTAL INSURANCE REQUIREMENTS.....	84
I.18 MANDATORY WRITTEN DISCLOSURES	84
PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS.....	85
SECTION J - LIST OF ATTACHMENTS	85

PART I - THE SCHEDULE

SECTION B - SUPPLIES OR SERVICES AND PRICE/COSTS

B.1 PRICE SCHEDULE

Contract Line Item (CLIN)	Description	QTY	UNIT	UNIT COST	TOTAL COST
0001	Firm-Fixed-Price Line Item Ordering Periods 1 -5 <u>End User Devices</u> to be provided in accordance with (IAW) Attachment No. 002 (“End User Device Specifications”), Section J, and the Commodities Enterprise Contract (CEC) Performance Work Statement (PWS) set forth in Section C to include but not limited to Paragraphs 6.0, 6.1, 7.0, 9.0. Included in this line item are all costs associated with VA System Acceptance Testing (PWS Paragraph 7.0), Standard Warranty (PWS Paragraph 9.0) and all shipping costs. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. DELIVERY DATE: To be identified in each DO INSPECT/ACCEPT: Destination PRESERVATION/PACKAGING: IAW CEC PWS Paragraph 11.0 SHIP TO: To be identified in each DO FOB: Destination	TBD	EA	IAW Attachment No. 009	TBD
0002	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>End User Devices Standard Installation</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to,	TBD	EA	IAW Attachment No. 009	TBD

	Paragraphs 8.0. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. DELIVERY DATE: To be identified in each DO INSPECT/ACCEPT: Destination				
0003	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>End User Devices One (1)-Year Extended Standard Warranty</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraphs 9.0 and 9.1. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. PERIOD OF PERFORMANCE: To be identified in each DO INSPECT/ACCEPT: Destination	TBD	EA	IAW Attachment No. 009	TBD
0004	CLIN Deleted				
0005	Firm-Fixed-Price Line Item Ordering Periods 1 -5 <u>Mobile Tablets</u> to be provided IAW Attachment No. 003 (“Mobile Tablet Specifications”), Section J, and the CEC PWS set forth in Section C to include but not limited to Paragraphs 6.0, 6.2, 9.0. Included in this line item are all costs associated one (1)-year Standard Warranty (PWS Paragraph 9.0) and all shipping costs. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. DELIVERY DATE: To be identified in each DO INSPECT/ACCEPT: Destination PRESERVATION/PACKAGING: IAW CEC PWS Paragraph 11.0 SHIP TO: To be identified in each DO FOB: Destination	TBD	EA	IAW Attachment No. 009	TBD

0006	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>Mobile Tablets Standard Installation</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraph 8.0. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. DELIVERY DATE: To be identified in each DO DELIVERY DATE: TBD INSPECT/ACCEPT: Destination	TBD	EA	IAW Attachment No. 009	TBD
0007	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>Mobile Tablets One (1)-Year Extended Standard Warranty</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraphs 9.0 and 9.1. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. PERIOD OF PERFORMANCE: To be identified in each DO INSPECT/ACCEPT: Destination	TBD	EA	IAW Attachment No. 009	TBD
0008	CLIN Deleted				
0009	Firm-Fixed-Price Line Item Ordering Periods 1 -5 <u>Servers</u> to be provided in accordance with IAW Attachment No. 004 (“Server Specifications”), Section J, and the CEC PWS set forth in Section C to include but not limited to Paragraphs 6.0, 6.3, 9.0. Included in this line item are all costs associated with Standard and Premium Warranties (PWS Paragraph 9.0) and all shipping costs. Pricing for each Ordering	TBD	EA	IAW Attachment No. 009	TBD

	Period is outlined in Attachment No. 009 to this contract. DELIVERY DATE: To be identified in each DO INSPECT/ACCEPT: Destination PRESERVATION/PACKAGING: IAW CEC PWS Paragraph 11.0 SHIP TO: To be identified in each DO FOB: Destination				
0010	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>Servers Standard Installation</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraph 8.0. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. DELIVERY DATE: To be identified in each DO INSPECT/ACCEPT: Destination	TBD	EA	IAW Attachment No. 009	TBD
0011	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>Servers One (1)-Year Extended Standard Warranty</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraphs 9.0 and 9.1. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. PERIOD OF PERFORMANCE: To be identified in each DO INSPECT/ACCEPT: Destination	TBD	EA	IAW Attachment No. 009	TBD
0012	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>Servers One (1)-Year Extended Premium Warranty</u> to be provided IAW the CEC PWS set	TBD	EA	IAW Attachment No. 009	TBD

	forth in Section C, to include but not limited to, Paragraphs 9.0 and 9.1. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. PERIOD OF PERFORMANCE: To be identified in each DO INSPECT/ACCEPT: Destination				
0013	Firm-Fixed-Price Line Item Ordering Periods 1 -5 <u>Networking Appliances (Switches/Routers)</u> to be provided IAW Attachment Nos. 005 (“Networking Appliances – Switch Specifications”) and 006 (“Networking Appliances – Router Specifications”), Section J, and the CEC PWS set forth in Section C to include but not limited to Paragraphs 6.0, 6.4, 9.0. Included in this line item are all costs associated with Standard and Premium Warranties (PWS Paragraph 9.0) and all shipping costs. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. DELIVERY DATE: To be identified in each DO INSPECT/ACCEPT: Destination PRESERVATION/PACKAGING: IAW CEC PWS Paragraph 11.0 SHIP TO: To be identified in each DO FOB: Destination	TBD	EA	IAW Attachment No. 009	TBD
0014	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>Networking Appliances (Switches/Routers) Standard Installation</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraph 8.0. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract.	TBD	EA	IAW Attachment No. 009	TBD

	DELIVERY DATE: To be identified in each DO INSPECT/ACCEPT: Destination				
0015	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>Networking Appliances (Switches/Routers) One (1)-Year Extended Standard Warranty</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraphs 9.0 and 9.1. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. PERIOD OF PERFORMANCE: To be identified in each DO INSPECT/ACCEPT: Destination	TBD	EA	IAW Attachment No. 009	TBD
0016	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>Networking Appliances (Switches/Routers) One (1)-Year Extended Premium Warranty</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraphs 9.0 and 9.1. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. PERIOD OF PERFORMANCE: To be identified in each DO INSPECT/ACCEPT: Destination	TBD	EA	IAW Attachment No. 009	TBD
0017	Firm-Fixed-Price Line Item Ordering Periods 1 -5 <u>Storage Arrays/Storage Appliances</u> to be provided IAW Attachment No. 007 (“Storage Arrays/Storage Appliance Specifications”), Section J, and the CEC PWS set forth in Section C to include but not limited to Paragraphs 6.0, 6.5, 9.0. Included in this line item are all costs associated with Standard and Premium Warranties (PWS Paragraph 9.0) and all	TBD	EA	IAW Attachment No. 009	TBD

	shipping costs. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. DELIVERY DATE: To be identified in each DO INSPECT/ACCEPT: Destination PRESERVATION/PACKAGING: IAW CEC PWS Paragraph 11.0 SHIP TO: To be identified in each DO FOB: Destination				
0018	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>Storage Arrays/Storage Appliances Standard Installation</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraph 8.0. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. DELIVERY DATE: To be identified in each DO INSPECT/ACCEPT: Destination	TBD	EA	IAW Attachment No. 009	TBD
0019	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>Storage Arrays/Storage Appliances One (1)-Year Extended Standard Warranty</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraphs 9.0 and 9.1. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. PERIOD OF PERFORMANCE: To be identified in each DO INSPECT/ACCEPT: Destination	TBD	EA	IAW Attachment No. 009	TBD
0020	Firm-Fixed-Price Line Item	TBD	EA	IAW Attachment	TBD

	Ordering Periods 1 – 5 <u>Storage Arrays/Storage Appliances One (1)-Year Extended Premium Warranty</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraphs 9.0 and 9.1. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. PERIOD OF PERFORMANCE: To be identified in each DO INSPECT/ACCEPT: Destination			No. 009	
0021	Firm-Fixed-Price Line Item Ordering Periods 1 -5 <u>Security Platforms</u> to be provided IAW Attachment No. 008 (“Security Platform Specifications”), Section J, and the CEC PWS set forth in Section C to include but not limited to Paragraphs 6.0, 6.6, 9.0. Included in this line item are all costs associated with Standard and Premium Warranties (PWS Paragraph 9.0) and all shipping costs. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. DELIVERY DATE: To be identified in each DO INSPECT/ACCEPT: Destination PRESERVATION/PACKAGING: IAW CEC PWS Paragraph 11.0 SHIP TO: To be identified in each DO FOB: Destination	TBD	EA	IAW Attachment No. 009	TBD
0022	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>Security Platforms Standard Installation</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraph 8.0. Pricing for each Ordering Period is outlined in Attachment No. 009 to this	TBD	EA	IAW Attachment No. 009	TBD

	contract. DELIVERY DATE: To be identified in each DO INSPECT/ACCEPT: Destination				
0023	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>Security Platforms One (1)-Year Extended Standard Warranty</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraphs 9.0 and 9.1. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. PERIOD OF PERFORMANCE: To be identified in each DO INSPECT/ACCEPT: Destination	TBD	EA	IAW Attachment No. 009	TBD
0024	Firm-Fixed-Price Line Item Ordering Periods 1 – 5 <u>Security Platforms One (1)-Year Extended Premium Warranty</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraphs 9.0 and 9.1. Pricing for each Ordering Period is outlined in Attachment No. 009 to this contract. PERIOD OF PERFORMANCE: To be identified in each DO INSPECT/ACCEPT: Destination	TBD	EA	IAW Attachment No. 009	TBD
0025	Time-and-Materials Line Item Ordering Periods 1 – 5 <u>Incidental Technical Support Services</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraphs 5.1.12, 10.0, 10.1, 10.2, 10.3 and all subparagraphs thereto. Specific requirements and pricing shall be established at the DO level. Labor categories and loaded labor rates applicable to performance under this line item	TBD	LO	IAW Attachment No. 010	TBD

	are outlined in Attachment No. 010 (“T&M Labor Rates”). PERIOD OF PERFORMANCE: To be identified in each DO INSPECT/ACCEPT: Destination				
0026	Ordering Periods 1 - 5 <u>Program Management and Reporting</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraphs 5.0, 5.1 and all subparagraphs thereto. Data Items associated with Program Management and Reporting are outlined in SLINS 0026AA and 0026AN. PERIOD OF PERFORMANCE: Date of Award through expiration of last active DO INSPECT/ACCEPT: Destination FOB: Destination				
0026AA	<u>Post Award Conference Meeting Minutes</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraph 5.1.1. This requirement is a <u>contract specific requirement</u> and shall be ordered on a one (1)-time basis in the first DO issued under the contract. DELIVERY DATE: No later than (NLT) ten (10) days after conclusion of the Contract Post Award Conference SHIP TO: IAW CEC Paragraph 5.1.1 INSPECT/ACCEPT: Destination FOB: Destination	1	EA	NSP	NSP

0026AB	<u>Action Item Summary</u> (Contract Post Award Conference) to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraph 5.1.1. This requirement is a <u>contract specific requirement</u> and shall be ordered on a one (1)-time basis in the first DO issued under the contract. DELIVERY DATE: NLT ten (10) days after conclusion of the Contract Post Award Conference SHIP TO: IAW CEC Paragraph 5.1.1 INSPECT/ACCEPT: Destination FOB: Destination	1	EA	NSP	NSP
0026AC	<u>Initial Draft Contract Level Work Plan and Schedule</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraph 5.1.1. This requirement is a <u>contract specific requirement</u> and shall be ordered on a one (1)-time basis in the first DO issued under the contract. DELIVERY DATE: IAW CEC PWS Paragraph 5.1. SHIP TO: To be presented at Contract Post Award Conference INSPEC/ACCEPT: Destination FOB: Destination	1	LO	NSP	NSP
0026AD	<u>Program Review Minutes</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraph 5.1.3. This requirement is a <u>contract specific requirement</u> and shall be ordered on a one (1)-time basis in the first DO issued under the contract. DELIVERY DATE: NLT ten (10) days after conclusion of the (quarterly) Contract Level Program Review SHIP TO: IAW CEC PWS Paragraph 5.1.3 INSPEC/ACCEPT: Destination FOB: Destination	1	LO	NSP	NSP

0026AE	<u>Action Item Summary (Program Reviews)</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraph 5.1.3. This requirement is a recurring <u>contract specific requirement</u> and shall be ordered on a one (1)-time basis in the first DO issued under the contract. DELIVERY DATE: NLT ten (10) days after conclusion of the (quarterly) Contract Level Program Review SHIP TO: IAW CEC PWS Para 5.1.3 INSPEC/ACCEPT: Destination FOB: Destination	1	LO	NSP	NSP
0026AF	<u>Updated Contract Level Work Plan and Schedule</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraph 5.1.3. This requirement is a <u>contract specific requirement</u> and shall be ordered on a one (1)-time basis in the first DO issued under the contract. DELIVERY DATE: NLT ten (10) days after conclusion of the (quarterly) Contract Level Program Review SHIP TO: IAW CEC PWS Paragraph 5.1.3 INSPEC/ACCEPT: Destination FOB: Destination	1	LO	NSP	NSP
0026AG	<u>Project Management Plan and Updates</u> to be provided IAW the CEC set forth in Section C, to include but not limited to, PWS Paragraph 5.1.4. This requirement is a <u>DO specific requirement</u> and shall apply only to the DO under which it is ordered. DELIVERY DATE: NLT ten (10) days after DO award. Updates to be provided on an “as required” basis. SHIP TO: IAW CEC PWS Paragraph 5.1.4 INSPEC/ACCEPT: Destination	1	LO	NSP	NSP

	FOB: Destination				
0026AH	<u>Monthly Progress Reports</u> to be provided IAW the CEC set forth in Section C, to include but not limited to, PWS Paragraph 5.1.5. This requirement is a <u>DO specific requirement</u> and shall apply only to the DO under which it is ordered. DELIVERY DATE: To be submitted on a monthly basis NLT five (5) days after the end of the preceding month SHIP TO: IAW CEC PWS Paragraph 5.1.5 INSPEC/ACCEPT: Destination FOB: Destination	1	LO	NSP	NSP
0026AJ	<u>CEC Ordering Portal Information and Updates</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraphs 5.1.6 and 5.1.8. This requirement is a <u>contract specific requirement</u> and shall be ordered on a one (1)-time basis in the first DO issued under the contract. DELIVERY DATE: Initial submission NLT ten (10) days after contract award. Updates to be submitted on an “as required” basis from date of contract award through expiration of last active DO SHIP TO: IAW CEC PWS Paragraph 5.1.6 and 5.1.8 INSPEC/ACCEPT: Destination FOB: Destination	1	LO	NSP	NSP
0026AK	<u>Catalog</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraph 5.1.6. This is a <u>contract specific requirement</u> and shall be ordered on a one (1)-time basis in the first DO issued under the contract. DELIVERY DATE: To be submitted NLT ten (10) days after contract award	1	LO	NSP	NSP

	SHIP TO: IAW CEC PWS Paragraph 5.1.6 INSPEC/ACCEPT: Destination <u>FOB</u> : Destination				
0026AL	<u>Change Management Plan</u> to be provided IAW the CEC PWS set forth in Section C, to include but not limited to, Paragraph 5.1.7. This requirement is a <u>contract specific requirement</u> and shall be ordered on a one (1)-time basis in the first DO issued under the contract. DELIVERY DATE: NLT thirty (30) days after award SHIP TO: Electronic submission to the COTR INSPEC/ACCEPT: Destination FOB: Destination	1	LO	NSP	NSP
0026AM	<u>Technology Refresh Engineering Change Proposal</u> to be provided IAW Attachment No. 001 (“Engineering Change Proposal”) and the CEC PWS set forth in Section C to include but not limited to Paragraph 5.1.8. This requirement is a <u>contract specific requirement</u> and shall be ordered on a one (1)-time basis in the first DO issued under the contract. DELIVERY DATE: As required, NLT thirty (30) days prior to product end-of-life SHIP TO: Electronic submission to the COTR and CO INSPEC/ACCEPT: Destination FOB: Destination	1	LO	NSP	NSP
0026AN	<u>Technology Insertion Engineering Change Proposal</u> to be provided IAW Attachment No. 001 and the CEC set forth in Section C, to include but not limited to, PWS Paragraph 5.1.9. This requirement is a <u>contract specific requirement</u> and shall be ordered on a one (1)-time basis in the first DO issued under the contract. DELIVERY DATE: As required IAW	1	LO	NSP	NSP

	Paragraph 5.1.9 SHIP TO: Electronic submission to the COTR and CO INSPEC/ACCEPT: Destination FOB: Destination				
--	--	--	--	--	--

SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK



PERFORMANCE WORK STATEMENT (PWS)

**DEPARTMENT OF VETERANS AFFAIRS
Office of Information & Technology**

Commodities Enterprise Contract (CEC)

Date: November 29, 2012

PWS Version Number: 21

Contents

<u>1.0 BACKGROUND</u>	26
<u>2.0 APPLICABLE DOCUMENTS</u>	26
<u>3.0 SCOPE OF WORK</u>	27
<u>4.0 PERFORMANCE DETAILS</u>	27
4.1 <u>PERFORMANCE PERIOD</u>	27
4.2 <u>PLACE OF PERFORMANCE</u>	28
4.3 <u>TRAVEL</u>	28
<u>5.0 SPECIFIC TASKS AND DELIVERABLES</u>	28
5.1 <u>PROGRAM MANAGEMENT AND REPORTING</u>	28
5.1.1 <u>Contract Post Award Conference</u>	29
5.1.2 <u>Delivery Order Kickoff Meetings</u>	29
5.1.3 <u>Program Reviews</u>	29
5.1.4 <u>Project Management Plan</u>	30
5.1.5 <u>Monthly Progress Reports</u>	30
5.1.6 <u>CEC Ordering Portal/Product Catalog/Delivery Order Tracking</u>	31
5.1.7 <u>Change Management Plan</u>	32
5.1.8 <u>Technology Refresh</u>	32
5.1.9 <u>Technology Insertion</u>	33
5.1.10 <u>Incidental Software</u>	33
5.1.11 <u>Incidental Hardware</u>	34
5.1.12 <u>Incidental Services</u>	34
<u>6.0 TECHNICAL FUNCTIONAL AREAS</u>	34
6.1 <u>END USER DEVICES</u>	34
6.2 <u>MOBILE TABLETS</u>	35
6.3 <u>SERVERS</u>	36
6.4 <u>NETWORKING APPLIANCES</u>	36
6.5 <u>STORAGE ARRAYS/STORAGE APPLIANCES</u>	36
6.6 <u>SECURITY PLATFORMS</u>	36
<u>7.0 VA SYSTEM ACCEPTANCE TESTING</u>	36
<u>8.0 STANDARD INSTALLATION (CONUS ONLY)</u>	37
<u>9.0 WARRANTY SUPPORT (IT HARDWARE AND INCIDENTAL SOFTWARE)</u>	39
9.1 <u>WARRANTY REPAIR:</u>	43
<u>10.0 INCIDENTAL TECHNICAL SUPPORT SERVICES</u>	44
10.1 <u>PRE-DEPLOYMENT SUPPORT SERVICES</u>	44
10.1.1 <u>Site Surveys</u>	44
10.2 <u>INSTALLATION AND INITIALIZATION SUPPORT</u>	44
10.2.1 <u>Custom Installation, Design and Configuration</u>	44
10.3 <u>POST-DEPLOYMENT SUPPORT SERVICES</u>	44
10.3.1 <u>Training Support</u>	44
10.3.2 <u>Application Support</u>	44
10.3.3 <u>Incidental Software Licenses</u>	45

<u>11.0 PACKAGING, HANDLING, STORAGE & TRANSPORTATION</u>	45
<u>12.0 VA DELIVERY ACCEPTANCE</u>	46
<u>13.0 GENERAL REQUIREMENTS</u>	46
<u>13.1 ENTERPRISE AND IT FRAMEWORK</u>	46
<u>13.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS</u>	46
<u>13.3 METHOD AND DISTRIBUTION OF DELIVERABLES</u>	50
<u>13.4 PERFORMANCE METRICS</u>	50
<u>13.5 FACILITY/RESOURCE PROVISIONS</u>	51
<u>ADDENDUM A</u>	52
<u>ADDENDUM B</u>	56

1.0 BACKGROUND

The Department of Veterans Affairs (VA) maintains a complex information technology (IT) enterprise architecture. The VA is seeking to establish a Commodities Enterprise Contract (CEC) arrangement that will ensure standardization of commercial IT hardware and associated installation, configuration, warranty, maintenance and technical support services solutions across the VA Enterprise. The task requirements described herein seek to not only ensure standardization, but interoperability with existing hardware infrastructure, while also leveraging the VA's purchasing power as a large enterprise. The IT Hardware Commodity purchases contemplated for this effort are as follows: end user devices (such as laptops and thin clients), mobile tablets, servers, networking appliances (switches/routers), storage arrays/storage appliances, and security platforms; all of which are as identified in Section 6.0 and detailed in the applicable technical specifications attached hereto. Although not required, the Government desires that Offerors propose (1) Original Equipment Manufacturer (OEM) for those products identified in PWS paragraphs 6.4 and 6.6, and as minimal OEMs as possible for those products identified in PWS paragraph 6.1. However, Offerors shall propose one (1) OEM for those products identified in PWS paragraphs 6.3 and 6.5. Additionally, the following services are also contemplated: installation, warranty support, and incidental technical support services such as site surveys, custom installation, training, and application support.

2.0 APPLICABLE DOCUMENTS

Documents referenced in or applicable to this Performance Work Statement (PWS) are listed below. In the performance of the tasks associated with this PWS, the Contractor shall comply with the following:

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002."
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules."
3. FIPS Pub 201, "Personal Identity Verification of Federal Employees and Contractors," March 2006.
4. 10 U.S.C. § 2224, "Defense Information Assurance Program."
5. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974."
6. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964."
7. Department of Veterans Affairs (VA) Directive 0710, "Personnel Suitability and Security Program," September 10, 2004.
8. VA Directive 6102, "Internet/Intranet Services," July 15, 2008.
9. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003.
10. OMB Circular A-130, "Management of Federal Information Resources," November 28, 2000.
11. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)."
12. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, March 2005.
13. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998.
14. Homeland Security Presidential Directive (12) (HSPD-12).
15. VA Directive 6500, "Information Security Program," August 4, 2006.

16. VA Handbook 6500, "Information Security Program," September 18, 2007.
17. VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle.
18. VA Handbook 6500.6, "Contract Security," March 12, 2010.
19. Program Management Accountability System (PMAS) portal (reference PWS References - Technical Library at <https://www.voa.va.gov/>).
20. ProPath Process Methodology (reference PWS References -Technical Library and ProPath Library links at <https://www.voa.va.gov/>) NOTE: In the event of a conflict, ProPath takes precedence over other processes or methodologies.
21. Technical Reference Model (TRM) (reference at <http://www.ea.oit.va.gov/Technology.asp>).
22. National Institute Standards and Technology (NIST) Special Publications.

3.0 SCOPE OF WORK

The VA requires commercial IT solutions (comprised of hardware and incidental services) to improve efficiency and productivity. The VA seeks to take advantage of technological advances and new business practices that promise to increase productivity and/or reduce costs while ensuring interoperability with the VA's existing hardware infrastructure. The task requirements described herein shall support the IT needs of VA programs, Initiatives, and other requirements throughout the VA enterprise. The IT Hardware commodities included in this acquisition consist of end user devices (such as laptops and thin clients), mobile tablets, servers, networking appliances (switches/routers), storage arrays/storage appliances, and security platforms; all of which are discussed in Section 6.0 and detailed in the applicable technical specifications attached hereto. Ancillary and/or incidental hardware, software, and services required for successful implementation may be acquired via any resulting contract vehicle and are detailed in Sections 9.0, and 10.0 of this document. The VA may purchase IT Hardware Commodity items or total IT solutions. All IT Hardware Commodity items shall be available for purchase. No leasing is contemplated by this acquisition. As VA's Enterprise Architecture continues to evolve, changes and/or updates to the products offered may be necessary to ensure compliance with Enterprise Architecture approved initiatives. These changes and updates will be incorporated into CEC through Technology Refresh and/or Technology Insertion, which are discussed in paragraphs 5.1.8 and 5.1.9, respectively.

4.0 PERFORMANCE DETAILS

This is a competitive acquisition for the award of multiple Indefinite Delivery, Indefinite Quantity (IDIQ) Contracts from which Firm Fixed Priced and/or Time and Materials Delivery Orders, or a combination thereof, shall be competed and issued, unless an exception to fair opportunity is otherwise justified.

4.1 PERFORMANCE PERIOD

The ordering period for the IT Hardware Commodity products and services described herein shall be for five (5) years from date of award. However, because performance of each Delivery Order awarded prior to Contract expiration may require continued warranty and technical support services as described in Section 9.0, warranty technical support services may be performed for a maximum of five (5) years after the expiration of the five (5) year ordering period.

Any work at any designated Government site in individual orders shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO).

There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that the VA follows:

Under current definitions, four (4) are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then the preceding Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then the Monday immediately thereafter shall be observed as a holiday.

The other six (6) are set by a day of the week and month:

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

The products will be delivered to, and used at, VA locations throughout the fifty (50) states; San Juan, Puerto Rico; and/or Manila, Philippines. Incidental services required under any resulting contract(s) may be performed at any VA facility throughout these locations. A listing of specific VA locations, for informational purposes, only, may be found at <http://www1.va.gov/directory/guide/home.asp?isFlash=1>.

Delivery locations will be specified in any resulting, individual Delivery Orders.

4.3 TRAVEL

The Government anticipates that travel will be required for performance of various task requirements described herein. Program Management (PM) travel for Contract level tasks will not be directly reimbursed by the Government and shall be included in the Offeror's Firm Fixed Price for IT Hardware Commodity Products. PM task requirements supporting Time and Materials (T&M) efforts may be captured at the Delivery Order level. In the event that additional travel is required, these requirements and costs shall be specified and the terms negotiated at the Delivery Order level. Travel for Standard Installation and Warranty shall be captured in the Offeror's Firm Fixed Prices for Standard Installation and Warranty, respectively. For any travel in Time and Material Delivery Orders these shall be captured as Other Direct Costs (ODCs).

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor, which for purposes of this document shall encompass the prime Contractor and all subcontractors, shall perform the following tasks:

5.1 PROGRAM MANAGEMENT AND REPORTING

The Contractor shall provide program management support at the both the Contract and Delivery Order level. This Program Manager or Program Management Team shall work closely with the Government to

manage contractual and programmatic issues that arise during performance of the Contract. The Contractor PM shall be responsible for the execution of all Contract tasks to include, but not be limited to: program reviews; kickoff meetings; status updates; various reporting requirements; and day-to-day concerns.

5.1.1 CONTRACT POST AWARD CONFERENCE

The Contractor shall coordinate and administer a Contract Post Award Conference at the Contractor's facility with key stakeholders and subject matter experts (SMEs), all of whom shall be identified by the VA Office of Information Technology (OIT) Project Manager (PM). The Contractor shall schedule the Conference within ten (10) business days after contract award or as agreed upon between the VA Contracting Officer's Technical Representative (COTR), the CO, and the Contractor. At the Conference, the Contractor shall present the details of the intended approach for managing the Contract, including an Initial Draft Contract Level Work Plan and Schedule to support the quarterly Contract Level Program Review requirements described in paragraph 5.1.3 below. All the key Contractor personnel shall be present for this initial review. Side meetings shall be held to allow for further in-depth discussion of the various program areas as necessary. The Contractor shall provide Post Award Conference Meeting Minutes and an Action Item Summary electronically to the COTR and all meeting participants no later than ten (10) days after conclusion of the Contract Post Award Conference.

Deliverables:

- A. Post Award Conference Meeting Minutes
- B. Action Item Summary
- C. Initial Draft Contract Level Work Plan and Schedule

5.1.2 DELIVERY ORDER KICKOFF MEETINGS

If required by the COTR and/or CO, the Contractor shall participate in kickoff meetings to be procured at the Delivery Order level. The purpose of this meeting is for the Contractor to brief the Government on how it intends to meet all the requirements of the Delivery Order. At the Government's election, the kickoff meetings may be held on-site at the Contractor's facility, Government facility, or by telephone conference. Specific requirements will be detailed in the individual Delivery Orders.

5.1.3 PROGRAM REVIEWS

The Contractor shall conduct Contract Level Program Reviews on a quarterly basis. At the Government's election, the Program Reviews may be held on-site at the Contractor's facility, Government facility, or by telephone conference. These Program Reviews shall address and provide in-depth information on program progress and all functions summarized by Delivery Order(s) to include, but not be limited to:

- 1. Administration
- 2. Schedule
- 3. Configuration Management
- 4. Technology Refresh / Insertion Products
 - Summary of tech insertion/refresh activities
 - Provide a technology roadmap identifying product lifecycle milestones, new technologies and product end-of-life (EOL) replacement strategies
- 5. Logistics

6. Testing
7. Quality Assurance
8. Field Support
9. Customer Issues and Resolutions

The Contractor shall provide Program Review Minutes, Action Item Summary, and an updated Contract Level Work Plan and Schedule, electronically, to the COTR and all meeting participants no later than ten (10) days after conclusion of the Contract Level Program Review.

Deliverables:

- A. Program Review Minutes
- B. Action Item Summary
- C. Updated Contract Level Work Plan and Schedule

5.1.4 PROJECT MANAGEMENT PLAN

If required by the individual Delivery Order, the Contractor shall provide a Project Management Plan (PMP) specifying the approach, timeline, and tools to be used in execution of the Delivery Order. The PMP shall include the risk, quality and technical management approach, detailed master schedule and milestones, project change control method, and proposed personnel. The Contractor shall keep the PMP current throughout the Delivery Order period of performance. The PMP shall take the form of both a narrative and graphic format that addresses the requirements discussed above. The PMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as specified within the Delivery Order. The initial PMP shall be delivered electronically to the COTR no later than ten (10) days after award of the Delivery Order. Updates are to be provided on an as-needed basis.

Deliverables:

- A. Project Management Plan and Updates

5.1.5 MONTHLY PROGRESS REPORTS

If required by the individual Delivery Order, the Contractor shall submit a Monthly Progress Report (MPR) via electronic mail. The MPRs shall address project status, including all work completed during the reporting period and work planned for the subsequent reporting period. The MPR shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation. The Contractor shall monitor performance against the PMP (if applicable) and report any deviations. It is expected that the Contractor shall maintain communication with the VA so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

The Contractor shall provide the COTR with MPRs in electronic form in Microsoft Word and Project formats no later than five (5) days after the end of the preceding month. These reports shall reflect data as of the last day of the preceding month.

The MPR shall include, but not be limited to, the following items:

1. Project status and progress summary by Delivery Order
2. Summary of equipment delivered and/or installed/de-installed that month
3. Summary of repairs, including date/time/location of repair and whether repair was accomplished on-time
4. Significant open issues, risk and mitigation action
5. Summary of problems resolved
6. Subcontractor performance – discuss 1st tier subcontractors and vendor performance
7. Schedule status
8. Status of required background investigations
9. Invoices, by Contract Line Item Number (CLIN), submitted and payments received to date
10. Warranty Information
11. License Information
12. Any other areas as specifically identified by the VA as detailed in the individual Delivery Orders

Monthly reports shall not contain security related information.

Deliverables:

- A. Monthly Progress Report

5.1.6 CEC ORDERING PORTAL/PRODUCT CATALOG/DELIVERY ORDER TRACKING

The Government will establish and maintain a web-based ordering portal. Ten (10) days after contract award, the Contractor shall provide the Government with CEC Ordering Portal information for all Contractor IT Hardware Commodities offered. This information shall include, but not be limited to:

1. Vendor IT Hardware Commodity Item Specification Sheet
2. Incidental Software (SW) and Hardware (HW) Dependencies
3. Manufacturer
4. Manufacturer Part Numbers
5. Unit Prices
6. Product Description

After receipt of approval from the CO, the Contractor shall provide updated information for the portal to reflect changes in products, prices, and notify and replace products reaching EOL with the newly refreshed and inserted products.

The CEC Ordering Portal will also be used as a Delivery Order Tracking System up to the point of, and including, delivery of the products. Therefore, the Contractor shall also provide up-to-date, information as necessary on the CEC Ordering Portal including, but not limited to:

1. Procurement / Delivery Date
2. Electronic Contract Management System (eCMS) Contract/ Order Number
3. Integrated Funds Distribution Control Point Activity Accounting & Procurement (IFCAP)
Purchase Order Number
4. VA Delivery Site Code (if applicable)
5. VA Delivery Site Mailing Address
6. Equipment Model Listing
7. Equipment Serial Number Listing
8. Equipment Status up to and including delivery confirmation

9. Warranty Information
10. Incidental Software License Information
11. Toll Free Phone Number described in Paragraph 9.0

The CEC Ordering Portal will be used to present all IT Hardware Commodity products and incidental services offered by the CEC contract to customers as well as up-to-date status and tracking information from within a single Ordering Portal.

Where possible, the Contractor shall use electronic means to collect data to populate the portals and reduce paper (for example electronic signature pads) to validate delivery.

In addition, ten (10) days after award, the Contractor shall deliver a catalog to the COTR and CO detailing all IT Hardware Commodity products and prices offered by the Contractor in their proposal for the CEC Contract. The catalog shall also include identification of, and associated prices for, subcomponents/modules for the Servers, Networking Appliances, and Storage Arrays/Storage Appliances Technical Functional Areas. The Government reserves the right to purchase any and/or all subcomponents/modules as specified in the Contractor's catalog.

Deliverables:

- A. CEC Ordering Portal Information and Updates
- B. Catalog

5.1.7 CHANGE MANAGEMENT PLAN

The Contractor shall submit a Change Management Plan that details its process to manage changes to the hardware delivered under this Contract. This Plan must include all changes as described in PWS Attachment A ("Engineering Change Proposals") and describe the methods by which the Contractor validates that the hardware delivered to the Government meets the requirements of the Government's detailed specifications. These methods should include, but not be limited to, necessary performance testing procedures performed by the Contractor and/or necessary VA System Acceptance Testing described in paragraph 7.0. The Plan shall also include the methods by which the Contractor ensures all necessary hardware documentation is updated to adequately reflect these changes. The Change Management Plan shall be delivered electronically to the COTR no later than thirty (30) days after contract award. The Contractor is hereby advised that it shall not substitute hardware/equipment, or make any modifications thereto, which would result in any change to the vendor/Original Equipment Manufacturer (OEM) model or part number proposed, unless authorized, in writing, by the Contracting Officer (CO) through the Engineering Change Proposal (ECP) process.

Deliverables

- A. Change Management Plan

5.1.8 TECHNOLOGY REFRESH

The Contractor shall monitor all IT Hardware Commodity products provided under this Contract and notify the CO if any products are required to be changed or updated to accommodate the latest technology. If any IT Hardware Commodity products are approaching the end of their product lifetime (EOL) (e.g., if a vendor/ OEM will no longer be marketing, selling, or promoting a particular product, or limiting or ending support for said product) the Contractor shall provide notification and an ECP, as defined in PWS

Attachment A, to the Contracting Officer Technical Representative (COTR) and CO within thirty (30) days prior to the EOL date. Notification can be either via email or overnight mail. The Contractor shall update the CEC Ordering Portal within ten (10) days (as defined in Section 5.1.6) with product refresh information, upon Government approval. The Government reserves the right to reject any Contractor-proposed ECP, at no cost to the Government.

In performing technology refreshment, the Contractor shall maintain the same brand name items as identified in the original Contract to the maximum extent practical.

The following conditions shall be met in performing a technology refresh:

- a. The product(s) refreshed shall be fully compatible/backwards compatible with the originally provided product.
- b. The product(s) refreshed shall meet or exceed the mandatory technical requirements as stated in the applicable specifications.
- c. The product(s) refreshed shall be off-the-shelf configurations.
- d. The product prices proposed, and incorporated into any resulting contract, are binding and thereby establish the Government's maximum liability for said product over the life of the Contract. Therefore, the price of the product(s) refreshed, including support services, shall not exceed the price proposed and incorporated into the basic Contract, for the product being refreshed.
- e. All refreshed products shall comply with the VA Acceptance testing defined in Section 7.0 of this PWS.

Deliverables:

- A. Technology Refresh Engineering Change Proposal

5.1.9 TECHNOLOGY INSERTION

As new IT Hardware technologies are developed and used by the commercial industry or the Government, the VA and/or Contractor may identify these technologies, and propose necessary additions, modifications, upgrades, enhancements, and improvements to the proposed contract IT Hardware Commodity product items. The Contractor shall translate the technology insertion recommendation into a formal ECP for the CO's approval. The Government reserves the right to reject any Contractor-proposed ECP, at no cost to the Government.

All inserted products shall undergo VA Acceptance testing as defined in Section 7.0 of this PWS.

Deliverables:

- A. Technology Insertion Engineering Change Proposal

5.1.10 INCIDENTAL SOFTWARE

Stand alone purchasing of software licenses is not within the scope of this PWS. However, software licenses incidental to, and necessary for, the successful operation of IT Hardware commodities that are not a part of the VA Gold Image (as defined in Section 7.0) may be included in any resulting Delivery Orders on a Time and Materials basis. Any incidental software shall go through VA Pre-Certification and Acceptance testing and/or shall be allowed by the One-VA Technology Reference Model (www.va.gov/trm). Offerors are hereby advised that in the event of conflict between the One-VA TRM and the CEC Solicitation, the Solicitation documents take precedence.

5.1.11 INCIDENTAL HARDWARE

In order for proper installation and/or integration of IT Hardware commodities, incidental hardware may be required. These incidental hardware items may consist of, but are not limited to: subcomponents/modules; cables; cords; racks; wires; and peripherals. These items, with the exception of subcomponents/modules which shall be purchased on a Firm Fixed Price basis, will be identified in individual Delivery Orders on a Time and Materials basis and shall be directly related to hardware purchased under the CEC contract.

5.1.12 INCIDENTAL SERVICES

Services that are required for successful implementation of the IT Hardware commodities purchased may be acquired under the CEC Contract. These services shall be directly related to hardware purchased under the CEC contract vehicle. The services listed within Section 10.0 are within the scope of the Contract.

6.0 TECHNICAL FUNCTIONAL AREAS

The Contractor shall provide the following IT Hardware Commodities and all incidental hardware, software, services, and licenses to render the hardware operational. Incidental software required shall be specified in individual Delivery Orders. The Contractor shall provide all commercially available hardware documentation to include specifications, installation guides, user's manuals and/or any additional standard hardware documentation in hard copy, electronically, or both. Specific details and quantities shall be described in the individual Delivery Orders.

The Contractor shall provide only new equipment and new parts for the required products described herein. **ABSOLUTELY NO "GRAY MARKET GOODS" shall be provided under any Delivery Order.** Gray Market Goods are defined as genuine branded goods sold outside of an authorized sales-territory (or by non-authorized dealers in an authorized territory) at prices lower than being charged in authorized sales territories (or by authorized dealers).

If software is required under a Delivery Order, the Contractor shall only provide the latest commercially available version unless authorized, in writing, by the CO.

6.1 END USER DEVICES

The Contractor shall provide End User Devices to facilitate information and data processing. Detailed specifications for each configuration tier are provided in PWS Attachment B, entitled "End User Devices Specifications." Although the Government desires as minimal OEMs as possible for those products identified in the table, below (e.g., a single OEM for Laptops compatible with a Windows operating system, a single OEM for the Monitors (both Small and Large)), the Contractor may provide one (1) OEM per End User device as referenced in the below table. The Contractor shall ensure that all end user devices are delivered pre-installed with the operating system required by the applicable delivery order, as well as the VA provided Gold Image as detailed in Section 7.0, unless otherwise stipulated in the individual Delivery Orders. The Gold Image will be distributed as Government Furnished Information (GFI) as detailed in the individual Delivery Orders.

Group 1: End User Devices (PWS 6.1)	Single OEM for Light Laptop compatible with Windows OS
--	--

	Single OEM for Docking Station that is compatible with the Offeror's proposed Light Laptop Single OEM for Medium Laptop compatible with Windows OS Single OEM for Docking Station that is compatible with the Offeror's proposed Medium Laptop Single OEM for Heavy Laptop compatible with Windows OS Single OEM for Docking Station that is compatible with the Offeror's proposed Heavy Laptop Single OEM for PC – Tablet compatible with Windows OS Single OEM for Docking Station that is compatible with the Offeror's proposed PC – Tablet Single OEM for – Monitors (Small) Single OEM for – Monitors (Large) Single OEM for – Laptops compatible with Mac OS (Medium, Heavy) Single OEM for Docking Station that is compatible with the Offeror's proposed Mac OS Laptops Single OEM for – Semi-Ruggedized Laptops compatible with Windows OS Single OEM for Docking Station that is compatible with the Offeror's proposed Semi-Rugged Laptop Single OEM for – Thin Clients compatible with Windows OS Single OEM for – Desktops compatible with Mac OS
--	---

6.2 MOBILE TABLETS

The Contractor shall provide Mobile Tablets to facilitate information/data processing and computing mobility across the VA. The five (5) Mobile Tablets required span three (3) configuration tiers and therefore, must be compatible with the following: Mac OS; Android OS; and Blackberry OS. Detailed specifications for each configuration tier are provided in PWS Attachment C, entitled "Mobile Tablet Specifications."

6.3 SERVERS

The Contractor shall provide Servers to facilitate information/data processing, network services, database management and warehousing, community collaboration, training, web services, and/or resource distribution (e.g., cloud computing) across the VA. The Servers span three (3) configuration tiers: Class A, Class B, and Class C (Rack/Blade). Detailed specifications for each configuration tier and for two (2) Chassis configurations are provided in PWS Attachment D, entitled “Server Specifications.” The Contractor shall provide products from a single OEM for all Class A/B/C Servers (Rack & Blade) and the two (2) Chassis configurations which meet the specification requirements.

6.4 NETWORKING APPLIANCES

The Contractor shall provide Switches and Routers to facilitate network connectivity and communication across the VA. The Switches span three (3) configuration tiers: Enterprise Class Modular LAN Campus Core Switch; Enterprise Class Stackable Network Access Switch; and Enterprise Class High Density Modular LAN Access Switch. The Routers consist of three (3) configuration Tiers: Class A; Class B; and Class C. Detailed specifications for all Switches and Routers configuration tiers are provided in PWS Attachment E, entitled “Switch Specifications,” and PWS Attachment F, entitled “Router Specifications.” Although the Government desires that all Networking Appliances be provided by a single OEM, the Contractor may provide Networking Appliances from more than one (1) OEM provided that each product meets the specification requirements.

6.5 STORAGE ARRAYS/STORAGE APPLIANCES

The Contractor shall provide Storage Arrays/Storage Appliances to facilitate data warehousing, management, sharing, and streaming across the VA. The Storage Arrays/Storage Appliances consist of thirteen (13) configuration tiers: Direct Attached Storage (DAS); Storage Area Network (SAN) Storage; Fibre Fabric SAN Switch; Network Attached Storage (NAS); Modular NAS Storage; Modular iSCSI Storage; LTO Tape Library; LTO Tape Cartridge; IP based Deduplication Storage; Virtual Tape Library (VTL) with Deduplication Storage; Unified Storage; Archive Storage; and GRID based Object Type Storage. Detailed specifications for each configuration tier are provided in PWS Attachment G, entitled “Storage Arrays/Storage Appliances.” The Contractor shall provide products from a single OEM, per each configuration tier that meet the specification requirements up to a possible total of thirteen (13) OEM’s if required.

6.6 SECURITY PLATFORMS

The Contractor shall provide security platforms to protect our Veterans personal information and protect the VA IT enterprise from cyber attacks and intrusion. The Security Platforms are comprised of three (3) products within one (1) configuration tier. Detailed specifications for the Security Platforms are provided in PWS Attachment H, entitled “Security Platform Specifications.” Although the Government desires that all Security Platforms within the configuration tier be provided by a single OEM, the Contractor may provide Security Platforms from more than one (1) OEM provided that each product meets the specification requirements.

7.0 VA SYSTEM ACCEPTANCE TESTING

In addition to the requisite operating system installed on the applicable end user device, VA will create a custom operating system image that will be named “VA Gold Image” for Contractor installation. The VA Gold Image shall be provided to the Contractor as GFI, after contract award to enable orders for End User Devices. Please be advised that contractors cannot participate in Delivery Order competitions that include

requirements for End-User devices requiring Gold Images until the End-User devices have passed VA acceptance testing. Image updates and/or testing of the current image will occur if/when the Contractor introduces new equipment models to VA over the life of the contract, or if a flaw is discovered in the VA Gold Image. Any device changes that take place within any current models will also need to go through the same testing of the drivers. The Gold Image will include only applications from current/future VA enterprise licensed software. In addition, once VA builds the Gold Image it will be delivered electronically to a secure file transfer protocol (FTP) site. The Contractor shall be responsible that a FTP site is established and hosted, at the Contractor's expense. The Contractor shall store all VA images securely at its site, in accordance with VA security and policies as depicted in PWS Addendum B. If issues arise with electronic transfer of the image, VA will pursue alternative physical transfer options with the Contractor.

Within ten (10) business days of receipt of a VA Gold Image and/or as part of every engineering change proposal (e.g., a new make/model/devices within a model due to technology refresh or insertion), the Contractor shall furnish, at no cost to VA, the proposed End User Device (one of each configuration) to VA's Pre Production Test facility located in Albany, NY and/or other VA-designated location. The VA Pre-Production Test Facility will test the equipment and image to ensure that it functions correctly within the current VA IT infrastructure; regression testing must take place involving VA application software to ensure that the VA-specific hard drive image is functioning correctly. The Government will complete product testing as soon as practicable, however, this regression testing requires a minimum of thirty (30) days for completion before items can be set to ship. Upon successful regression testing, VA will notify the Contractor that the image has passed testing, and the manufacturer may begin building the end user device VA has ordered using the accepted image. This imaging shall take place on the end user device assembly line and include appropriate burn-in time to ensure image integrity. The end user device manufacturer's standard device management and diagnostic software shall be provided to VA. If the proposed equipment fails to pass the Pre-Production testing, VA will return the devices that failed to the Contractor or designated manufacturer point of contact (at the Contractor's cost), and the Contractor shall provide new devices to the pre-production testing facility. If the test unit passes, the accepted test unit will be returned to the Contractor. VA reserves the right to reject any change proposal at no cost to VA.

As part of the VA Gold imaging process, all laptop Basic Input Output System (BIOS) must be set to Preboot Execution Environment (PXE) as first boot option, and hard drive controller set to Advanced Technology Attachment (ATA) (no Redundant Array of Independent Disks (RAID) enabled). VA reserves the right to change these settings, if desired, before any required delivery. The Contractor imaging process shall support Software Change and Configuration Management (SCCM) for Operating System Deployment (OSD) OEM images including proactive driver management and driver packs that are small and optimized for SCCM OSD, specifically. The Contractor shall support multiple image file formats, the main file format the VA uses is Windows Imaging Format (wim). The Contractor shall allow for created images to be applied seamlessly to systems at the factory during the manufacturing process. Acceptance testing for all other commodities will be completed in accordance with commercially established practices, at the VA site, unless otherwise provided for in individual Delivery Orders.

8.0 STANDARD INSTALLATION (CONUS ONLY)

The Contractor may be required to provide installation support for all IT Hardware Commodities listed in the Technical Function Areas, Section 6.0, as specified in individual Delivery Orders. The Contractor shall provide the standard documentation (e.g., User Manual, Operators Manual, Installation Guide, etc.) to support the installation of the new hardware. The Contractor shall validate successful operation of any installed products prior to acceptance.

The Contractor shall develop a master delivery schedule of equipment to all sites receiving delivery of

equipment as specified in each Delivery Order. This schedule shall include, at a minimum, current status of site delivery. Schedules shall be coordinated with the local designated point of contact (POC) for installation requirements for each site identified in the Delivery Order.

The Contractor shall install new equipment as indicated in each Delivery Order which may require installation of equipment after normal business hours. After-hours installation requirements will be defined in each Delivery Order and determined by each site on an installation-by-installation basis.

The Contractor shall abide by all local VA site policies and requirements regarding equipment delivery, installation and associated personnel. The Contractor shall be responsible for coordinating all deliveries by contacting the site prior to delivery to obtain knowledge of local constraints and policies, including security requirements both for equipment and personnel.

If the new equipment replaces an existing system, the Contractor shall disconnect the existing hardware and turn it over to local Government IT Operations staff for further disposition. The Contractor shall remove all storage devices (e.g., hard drives, flash memory, etc.) from replaced systems, annotate the VA identification number (EE number) and/or serial number of the new storage device and the VA identification number (EE number) and/or serial number of the replaced storage device, create a cross reference list for signature by the Information Security Officer (ISO), and turn the hard drive over to the local Government IT Operations staff.

When proposed Delivery Orders include Standard Installation requirements, the Contractor shall perform the following installation services:

1. The Contractor shall remove all packaging and waste associated with new equipment installations and dispose of accordingly. VA encourages the Contractor to use multipacks, if available.
2. The Contractor shall provide any necessary racks, mounts, brackets, installation kits, and/or cables necessary to install the required hardware to an operational state. Any incidental hardware shall be identified in the individual Delivery Orders based upon the selected Contractor's quote or proposal. Once the new hardware is installed and connected, the hardware shall be powered on, logged onto, and tested for network connectivity. Staging areas for IT Hardware commodities to be installed are usually available at most VA sites (availability and size will vary by site). The Contractor shall coordinate site staging areas with the site delivery POC as identified in the individual Delivery Order.
3. The Contractor shall prepare an Installation Certification Sheet and have the installation certified by the designated VA site installation POC. The Contractor shall insure the VA POC certifies the installation on the same day of installation, and the Contractor must deliver the Installation Certification Sheet to the Government IT Operations POC as specified in the Delivery Order.
4. If applicable, and as defined in the individual Delivery Order, the Contractor shall input VA asset identification information into the BIOS of each Desktop and/or Laptop. The method shall include both a central factory level assignment and a local VA site assignment capability.
5. The Contractor shall apply the Contractor service tag and serial number at the factory on the exterior of the equipment. The Contractor shall provide the serial numbers for each piece of equipment to the VA site installation POC and/or COTR no later than five (5) days prior to shipment to the site. Any further requirements for the service tag will be defined at the Delivery Order level.

6. The Contractor shall provide the necessary knowledge and support for installation of the IT Hardware Commodities across the local area network (LAN), virtual private network (VPN), and/or Wide Area Network (WAN) environments.
7. The Contractor shall provide support for IT hardware installation including applicable operating systems; installation of software; monitoring and adjusting system performance; application of latest hardware/software patches, security updates and service packs; and repairs and upgrades as necessary for installation of the IT Hardware Commodity.

All standard installation performed OCONUS will be deemed a custom installation in accordance with PWS paragraph 10.2.1.

9.0 WARRANTY SUPPORT (IT HARDWARE AND INCIDENTAL SOFTWARE)

The Contractor is responsible for warranty and warranty support. The Contractor shall provide, maintain, and administer warranty support agreements for use on all IT Hardware Commodities and incidental software, and shall provide extended warranty technical support at the level required in individual Delivery Orders. The Contractor shall be the primary/initial interface between the VA and the OEMs regarding all technical support issues as well as the primary interface for all warranty information.

Upon delivery of each IT Hardware Commodity, the Contractor shall pass through the applicable OEM warranty to the Government, at no additional cost to the Government. In addition, for all IT Hardware Commodities, the Contractor shall provide VA, for a period of no less than one (1) year from acceptance of the IT Hardware Commodity to the Government (except Storage Arrays/Storage Appliances, which is no less than three (3) years), the Standard or Premium Warranty, as defined below, as part of the purchase price. This Warranty shall run concurrently with any applicable pass through OEM warranty provided. The Government reserves the right to purchase additional one (1) year increments of either the Standard or Premium Warranty Support, as an Extended Warranty, for any IT Hardware Commodity Item. The Government can purchase an Extended Warranty, be it Standard or Premium Warranty Support, for an item, as outlined in the table below, at any time prior to the expiration of the then in-effect Warranty coverage period, for that item. However, if the then in-effect Warranty expires, it cannot be renewed. In no instance, however, shall Warranty Coverage and/or Support exceed five (5) years from the date a product is purchased.

Product Group	Standard Warranty	Premium Warranty
Group 1 – End User Devices		
Group A – Laptops Windows OS*	Unit price with 1 Year Warranty	Not Applicable
	Unit price with 2 Year Warranty	Not Applicable
	Unit price with 3 Year Warranty	Not Applicable
	Unit price with 4 Year Warranty	Not Applicable
Group B – Laptop MAC OS*	Unit price with 1 Year Warranty	Not Applicable
	Unit price with 2 Year Warranty	Not Applicable
	Unit price with 3 Year Warranty	Not Applicable
	Unit price with 4 Year Warranty	Not Applicable
Group C – Thin Clients	Unit price with 1 Year Warranty	Not Applicable

Group 2 – Mobile Tablets		
Groups A through C	Unit price with 1 Year Warranty	Not Applicable
Group 3 - Servers		
Group A – Rack Mounted/Blade	Unit price with 1 Year Warranty	Unit price with 1 Year Warranty
	Unit price with 2 Year Warranty	Unit price with 2 Year Warranty
	Unit price with 3 Year Warranty	Unit price with 3 Year Warranty
	Unit price with 4 Year Warranty	Unit price with 4 Year Warranty
	Unit price with 5 Year Warranty	Unit price with 5 Year Warranty
Group 4 – Networking Appliances		
Group A – Routers/Switches	Unit price with 1 Year Warranty	Unit price with 1 Year Warranty
	Unit price with 2 Year Warranty	Unit price with 2 Year Warranty
	Unit price with 3 Year Warranty	Unit price with 3 Year Warranty
	Unit price with 4 Year Warranty	Unit price with 4 Year Warranty
	Unit price with 5 Year Warranty	Unit price with 5 Year Warranty
Group 5 – Storage Arrays/Storage Appliances		
Groups A through K	Unit price with 3 Year Warranty	Unit price with 3 Year Warranty
	Unit price with 4 Year Warranty	Unit price with 4 Year Warranty
	Unit price with 5 Year Warranty	Unit price with 5 Year Warranty
Group 6 – Security Platforms		
Group A – Security Devices	Unit price with 1 Year Warranty	Unit price with 1 Year Warranty
	Unit price with 2 Year Warranty	Unit price with 2 Year Warranty
	Unit price with 3 Year Warranty	Unit price with 3 Year Warranty
	Unit price with 4 Year Warranty	Unit price with 4 Year Warranty
	Unit price with 5 Year Warranty	Unit price with 5 Year Warranty

*Note: Standard and Premium Warranty requirements do not apply to Docking Stations. Accordingly, Offerors are not required to provide these warranties with its proposed docking stations; Offerors shall only pass-through the applicable OEM warranty.

For Storage Arrays/Storage Appliances, this Standard or Premium Warranty shall be for a period of no less than three (3) years, shall be deemed part of the purchase price, and shall run concurrently with any applicable pass through OEM warranty provided. The Government reserves the right to purchase additional one (1) year increments of either the Standard or Premium Warranty Support, as an Extended Warranty for any storage array/storage appliance. The Government can purchase an Extended Warranty, be it Standard or Premium Warranty Support, for an item at any time prior to the expiration of the then in-effect Warranty coverage period, for that item. However, if the then in-effect Warranty expires, it cannot be renewed. In no instance, however, shall Warranty Coverage and/or Support exceed five (5) years from the date a product is purchased.

For all IT Hardware Commodities, the Warranty shall begin on the first day following the date the equipment is accepted by the Government in accordance with Paragraph 12.0. The Contractor may provide third (3rd) party warranties provided that OEM original and refurbished parts, along with OEM certified technicians, are utilized by the 3rd party vendor.

Warranty Technical Support Levels

The following defines the Standard Warranty Technical Support, and where applicable, the Premium Warranty Technical Support, required for each IT Hardware Commodity Group, which the Contractor shall provide when specified in individual Delivery Order requirements.

END USER DEVICES/MOBILE TABLETS

Standard Warranty

- Technical telephone and email support shall be available Monday – Friday (i.e., standard five (5) day business week) from 9:00 am to 5:00 pm local time of the impacted VA site. The Contractor shall provide a dedicated toll-free line that will route directly to a Contractor Tier 2 or 3 customer service/technical support representative, and not a Tier 1 help desk/support technician.
- The Contractor shall acknowledge the VA's request for warranty support, via email or call-back, within two (2) business hours of receipt, in accordance with the days and times specified above.
- Contractor's initial on-site or remote diagnosis shall be completed within one (1) business day.
- Following diagnosis, on-site labor/repair and/or part/product replacement shall be completed by the Contractor within the same or next business day.
- The Contractor shall have repaired or replaced all failing equipment, to fully operational status, by Close of Business (COB) on the second business day after diagnosis. The Contractor shall bear all shipping costs for replacement parts and replacement of the product.
- Twenty-four (24) hour access to Contractor or OEM provided web support/knowledge base.
- Access to all product/firmware microcode patches, updates, and upgrades.

Premium Warranty (N/A)

SERVERS/NETWORKING APPLIANCES (SWITCHES/ROUTERS)/ STORAGE ARRAYS - STORAGE APPLIANCES/SECURITY PLATFORMS

Standard Warranty

- Technical telephone and email support shall be available Monday – Friday (i.e., standard five (5) day business week) from 9:00 am to 5:00 pm local time of the impacted VA site. The Contractor shall provide a dedicated toll-free line that will route directly to a Contractor Tier 2 or 3 customer service/technical support representative, and not a Tier 1 help desk/support technician.
- The Contractor shall acknowledge the VA's request for warranty support, via email or call-back, within two (2) business hours of receipt, in accordance with the days and times specified above.

- Contractor's initial on-site or remote diagnosis shall be completed within one (1) business day.
- Contractor's initial attempt to repair shall be completed within one (1) business day following the Contractor's initial on-site or remote diagnosis. Contractor shall provide steady efforts to ensure that the product is restored to fully operational status.
- Each additional business day that the issue is unresolved shall result in the issue continuously being escalated to the next support level, until top level support is reached. The Contractor shall provide the VA with a clear escalation time-line from the Contractor's help desk support technician to the Chief Executive Officer (CEO), or otherwise equivalent highest level Officer.
- Twenty-Four (24) hour access to Contractor or OEM web support/knowledge base.
- Access to all product/firmware/ microcode patches, updates and upgrades.

Premium Warranty

- Technical telephone support shall be available twenty-four (24) hours X seven (7) days a week X 365 days a year. The Contractor shall provide a dedicated toll-free line that will route directly to a Contractor Tier 2 or 3 customer service/technical support representative, and not a VA Tier 1 help desk/support technician.
- Tier 2 or 3 response to VA's request for warranty support shall be made within fifteen (15) minutes of VA's initial contact.
- Contractor's initial on-site or remote diagnosis shall be completed within four (4) hours.
- Contractor's initial attempt to repair shall be completed within four (4) hours following the Contractor's initial on-site or remote diagnosis. Contractor shall provide steady efforts to ensure that the product is restored to fully operational status.
- Each four (4)-hour period that the issue is unresolved shall result in the issue continuously being escalated to the next support level, until top level support is reached. The Contractor shall provide the VA with a clear escalation time-line from the Contractor's help desk support technician to the Chief Executive Officer (CEO), or otherwise equivalent highest level Officer.
- Twenty-Four (24) hour access to Contractor or OEM web support/knowledge base.
- Access to all product/firmware/ microcode patches, updates and upgrades.

Regardless of whether the Contractor is providing Standard or Premium Warranty Technical Support, the VA will provide internal Tier 1 help desk support for the IT Hardware Commodity purchased under any resulting contract. The process flow is defined in PWS Attachment I, entitled "CEC Call Flow." The Contractor shall provide a dedicated toll-free line that will route directly to a Tier 2 customer

service/technical support representative versus a Tier 1 VA help desk/support technician. If the OEM and the Contractor are not the same, the Contractor is responsible to work through the escalation process. The Contractor shall provide a clear escalation time line and process through all levels of technical support.

Under both Standard and Premium Warranty Technical Support, the Contractor shall provide asset tracking information to the VA Tier 1 Help Desk for all IT Hardware Commodities. Data to be provided shall include, at a minimum:

1. eCMS Contract/order number
2. IFCAP Purchase Order Number
3. VA Delivery Site Code if applicable
4. VA Delivery Site Mailing Address
5. Equipment Model
6. Equipment Serial Number
7. Warranty Information
8. Hardware / Software License Information

9.1 WARRANTY REPAIR

The Contractor shall provide on-site warranty repair services in accordance with the timeframes set forth in the applicable technical support level specified in an individual Delivery Order. The Contractor shall repair or replace all failing equipment covered under the warranty. In the event that failing/defective equipment capable of storing VA data (e.g., hard drives, storage devices, mobile tablets, laptops, etc.) is replaced pursuant to the Warranty, the Contractor shall disconnect and/or remove the failing/defective equipment and turn said equipment over to local Government IT Operations Staff for disposition, and/or removal of VA data where possible. If authorized by the Government, failing/defective equipment that is replaced pursuant to the Warranty and is not capable of storing VA data, or from which all VA data has successfully been removed, shall be returned to the Contractor. All replacement items shall, at a minimum, assume the remaining warranty period of the original item replaced. The Contractor shall use OEM original and refurbished parts along with OEM certified technicians to perform any warranty repair. The Contractor shall bear all shipping costs for replacement parts. The Contractor shall only maintain spare parts inventories at VA locations when explicitly approved by the Government.

If the Contractor is not the manufacturer, the Contractor shall manage the service/support function. Additionally, the Contractor is responsible for ensuring that its own or any subcontractor-provided technical support does not void a pass through OEM warranty. If Contractor/Subcontractor provided technical support results in a warranty being voided, the Contractor will still be responsible for providing warranty support with no degradation in system operational status or availability to the VA. Certified VA IT Operations staff shall be authorized to repair faulty equipment on-site without voiding warranties purchased if this is deemed most expeditious to returning the unit to service. These repair services may be conducted by VA or VA contracted staff.

As stated previously, the Contractor shall make available Standard and Premium Extended Warranty coverage for the specified IT Hardware commodities in increments of one (1) year, where applicable, but in no event shall extended warranty coverage exceed five (5) years from date of the purchase of the IT

Hardware Commodity.

The Contractor shall provide a report of all warranties to the Government as detailed in the individual Delivery Orders and provide a listing of any warranties within 180 days of expiration as an attachment to the Monthly Progress Report.

10.0 INCIDENTAL TECHNICAL SUPPORT SERVICES

The following services shall be provided by the Contractor for required support above and beyond standard installation and warranty requirements identified in Sections 8.0 and 9.0 and as specifically identified in individual Delivery Orders. These incidental services will be reimbursed on a Time and Materials basis.

10.1 PRE-DEPLOYMENT SUPPORT SERVICES

10.1.1 SITE SURVEYS

When required, the Government will provide the Contractor access to VA sites to perform site surveys necessary to develop plans for the installation/initialization of the newly acquired hardware and associated incidental software. The Contractor shall take into account floor plans and layouts, existing IT systems, existing software systems and interfaces, existing cabling, power distribution, grounding, heating, ventilating, and air conditioning (HVAC) systems, access floor systems, lighting, backboards, and any other required GFE and materials.

If facility/structural alterations are required to support installation, all such alterations must be authorized and performed by the Government.

10.2 INSTALLATION AND INITIALIZATION SUPPORT

10.2.1 CUSTOM INSTALLATION, DESIGN AND CONFIGURATION

The Contractor shall provide custom installation, design and configuration support above and beyond standard installation requirements identified in Section 8.0 and as identified in the individual Delivery Orders. These services shall include but are not limited to technical areas such as system design, de-installation, data migration, and OCONUS installations.

10.3 POST-DEPLOYMENT SUPPORT SERVICES

10.3.1 TRAINING SUPPORT

The Contractor shall provide standard commercial training and other services related to installation, set-up, configuration and use of purchased equipment.

Training requirements shall be specified in individual Delivery Orders.

10.3.2 APPLICATION SUPPORT

Application support shall include support for installation, configuration, upgrading, patching, and/or debugging of all incidental software. If the Contractor is not the software manufacturer, the Contractor shall manage the service/support function.

If a software failure is suspected, the Contractor shall attempt to resolve the issue remotely in accordance with VA security standards and policies. If the software cannot be resolved remotely, the Contractor shall arrange for an on-site technician to be dispatched to resolve the issue. The Contractor shall repair or replace all failing incidental software as required by the terms of the applicable warranty unless otherwise specified in the individual delivery order. The Contractor shall bear all shipping costs.

Application Support requirements shall be specified in individual Delivery Orders.

10.3.3 INCIDENTAL SOFTWARE LICENSES

The Contractor shall provide licenses and support for incidental software as appropriate. The Contractor shall be responsible for providing licenses as detailed in individual Delivery Orders.

The Contractor shall provide a report of all licenses provided to the Government, as specified in the individual Delivery Orders.

11.0 PACKAGING, HANDLING, STORAGE AND TRANSPORTATION

The Contractor shall establish packaging, handling, storage and transportation processes and procedures to prevent damage and mishandling of the hardware, software and incidental items from acquisition through installation. The Contractor shall be liable for all damage, deterioration, and/or losses incurred during shipment, handling, storage and transportation unless the damage, deterioration, and/or losses are due to the fault of the Government.

The Contractor shall identify and report to the Government any unique or special packaging, handling, storage or transportation requirements.

The Contractor shall be responsible for transporting equipment and personnel required for installation to the installation site. Movement of equipment from the delivery site to the staging and installation locations may require vehicles with lift capability or machine transport carts. The Contractor shall provide its staff with vehicles, carts, trash, receptacles, and any other equipment or supplies necessary to carry out the requirements of each Delivery Order. VA anticipates, at a minimum, that carts will be required at all sites. Additional site requirements will be provided during pre-installation coordination with the sites and as specified in the individual Delivery Orders.

Unless otherwise specified, all items shall be preserved, packaged, and packed in accordance with standard commercial practices and in a manner that will afford protection against corrosion, deterioration and physical damage during shipment. The items shall be packed in a manner which conforms to the requirements of Uniform Freight Classification for rail shipment, National Motor Freight Classification for truck shipment, Parcel Post Regulations, and the regulations of other carriers as applicable to the mode of transportation employed.

Exterior shipping containers and items not shipped in containers shall be clearly marked on an external surface as follows:

- a) Delivery Point of Contact (POC) & Phone number
- b) Contract Number
- c) Delivery Order Number
- d) IFCAP Purchase Order Number
- e) Itemized list of contents including quantity and Contract Line Item Number (CLIN)

12.0 VA DELIVERY ACCEPTANCE

Each Delivery Order issued will have its own Acceptance Official. Unless otherwise specified within a Delivery Order, acceptance of all items delivered under the CEC Contract will take place at the VA site specified on each individual Delivery Order. The Contractor shall only tender for acceptance those items that conform to the requirements of the CEC Contract and Delivery Order under which delivery of IT Hardware Commodities are required. VA may request equipment be delivered to an individual facility without having the Contractor install the equipment. In these instances, VA will take responsibility for the equipment at the delivery location and free the Contractor from all responsibilities associated with initial equipment installation. In these instances, the date of acceptance shall be considered to be the date of equipment delivery.

13.0 GENERAL REQUIREMENTS

13.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one (1) component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the IT used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

As required and defined in the individual delivery orders the Contractor shall support VA efforts in accordance with the Program Management Accountability System (PMAS) that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for IT, PMAS is a VA-wide initiative to better empower the OI&T Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

ProPath is a VA-wide process management tool that builds upon the OI&T Program and Development managers' delivery of high-quality products, and provides an 'at-a-glance' perspective of nearly every step in the software development process. If applicable to the individual delivery order the Contractor shall utilize the tools and templates, and shall file documents in ProPath as a central resource as required by the VA PMAS Process.

13.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

The following security requirement must be adhered to regarding Contractor owned equipment used to support the VA. PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within the VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COTR, CO, the PM, and the ISO must be notified and verify all security requirements have been adhered to.

1. Information made available to the Contractor/Subcontractor by VA for the performance or

administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, Federal Acquisition Regulation (FAR) 52.227-14(d) (1).

2. VA information should not be co-mingled, if possible, with any other data on the Contractor/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor shall ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.
3. Prior to termination or completion of this contract, Contractor/Subcontractor shall not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the Contractor that the data destruction requirements above have been met shall be sent to the VA CO within thirty (30) days of termination of the Contract.
4. The Contractor/Subcontractor shall receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this Contract.
5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.
6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or for cause under Federal Acquisition Regulation (FAR) Part 12.
7. The Contractor/Subcontractor shall store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2

validated.

8. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.
9. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The Contractor/Subcontractor shall refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA CO for response.
10. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.
11. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Certification and Accreditation (C&A) or a Memorandum of Understanding-Interconnection Service Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COTR.
12. Position Sensitivity and Background Investigation - The position sensitivity and the level of background investigation commensurate with the required level of access is:

- ☐ Low/NACI
☐ Moderate/MB
☒ High/BI

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Security Suitability Program," Appendix A)
Low	National Agency Check with Written Inquiries (NACI) A NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.

Moderate	Minimum Background Investigation (MBI) A MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; and a verification of the educational degree.
High	Background Investigation (BI) A BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; and a verification of the educational degree.

Contractor Responsibilities:

- a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language. The Contractor shall provide the name, address, date of birth, Social Security Number and any other pertinent and relevant information of the Contractor personnel assigned to this project to the COTR and CO, as requested, and prior to the Delivery Order Level Kickoff Meetings.
- b. The Contractor shall bear the expense of obtaining background investigations. If the investigation is conducted by the Office of Personnel Management (OPM), the Contractor shall reimburse VA within thirty (30) days.
- c. The Contractor(s) and Contractor point of contact (POC) will receive an email notification from the Security and Investigation Center (SIC) identifying the website link that includes detailed instructions regarding completion of the background clearance application process and what level of background clearance was requested. Reminder notifications will be sent if the complete package is not submitted by the due date.
- d. The Contractor shall submit or have their personnel submit the required forms (SF 85P - Questionnaire for Public Trust Positions, SF 85P-S – Supplemental Questionnaire for Selected Positions, FD 258 – U.S. Department of Justice Fingerprint Applicant Chart, VA Form 0710 – Authority for Release of Information Form, Optional Form 306 – Declaration for Federal Employment, and Optional Form 612 – Optional Application for Federal Employment) to the VA Office of Security and Law Enforcement within thirty (30) calendar days of receipt.
- e. All costs associated with obtaining clearances for Contractor provided personnel shall be the responsibility of the Contractor. Further, the Contractor shall be responsible for the actions of all individuals provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
- f. If the security clearance investigation is not completed prior to the start date of the contract, the contract employee may work on the Contract with an initiated status while the security

clearance is being processed. However, the Contractor shall be responsible for the actions of the Contractor personnel it provides to perform work for the VA. In the event damage arises from work performed by Contractor personnel, under the auspices of the contract, the Contractor shall be responsible for resources necessary to remedy the incident.

- g. The investigative history for Contractor personnel working under this Contract must be maintained in the databases of either the OPM or the Defense Industrial Security Clearance Organization (DISCO).
- h. The Contractor, when notified of an unfavorable determination by the Government, shall withdraw the employee from consideration in working under the contract.
- i. Failure to comply with the Contractor personnel security requirements may result in termination of the contract for default.

13.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall be provided in contractor format and delivered in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007, MS Excel 2000/2003/2007, MS PowerPoint 2000/2003/2007, MS Project 2000/2003/2007, MS Access 2000/2003/2007, MS Visio 2000/2002/2003/2007, CAD 2002, and Adobe Postscript Data Format (PDF).

13.4 PERFORMANCE METRICS

The Contractor shall monitor performance against the established schedule, milestones, risks and resource support outlined in the approved PMP. The Contractor shall report any deviations in the Monthly Progress Report. As a minimum, the following metrics shall be included:

Performance Objective	Performance Standard	Acceptable Performance Levels	Surveillance Method
1. Technical Needs	Shows understanding of requirements Efficient and effective in meeting requirements Meets technical needs and mission requirements Offers quality services/products	Achieve 3.0 or higher	Performance Assessment
2. Project Milestones and Schedule	Quick response capability Products completed, reviewed, delivered in timely manner Notifies customer in advance of potential problems	Achieve 3.0 or higher	Performance Assessment
3. Project Staffing	Currency of expertise Personnel possess necessary knowledge, skills and abilities to	Achieve 3.0 or higher	Performance Assessment

	perform tasks		
4. Value Added	Provided valuable service to Government Services/products delivered were of desired quality	Achieve 3.0 or higher	Performance Assessment

Detailed Performance Metrics shall be identified in the individual Delivery Orders.

The contractor shall comply with IEEE 1680 "Standard for Environmental Assessment of Personal Computer Products"—also known as the Electronic Product Environmental Assessment Tool (EPEAT)—the first U.S. standard that provides guidelines for identifying environmentally friendly desktop and laptop computers and monitors. For more detailed information on the EPEAT criteria, visit <http://www.epeat.net/>. All End- User Devices (PWS section 6.1) provided under this contract, with the exception of docking stations, shall be rated EPEAT “Silver” or higher. Equipment provided on this contract is required to comply with EPA disposal standards.

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the support required by this PWS in an acceptable manner. The Government reserves the right to alter or change the QASP at its own discretion. A Performance Based Service Assessment Survey will be used in combination with the QASP to assist the Government in determining acceptable performance levels.

13.5 FACILITY/RESOURCE PROVISIONS

The Government shall provide office space, telephone service and system access required for authorized contract staff work at a Government location to accomplish the Tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis as specified in the Delivery Order.

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the COTR as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

The VA shall provide access to VA specific systems/network as required for execution of the task via a site-to-site VPN or other technology, including VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses. The Contractor shall utilize government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall In Accordance With (IAW) VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. For detailed Security and Privacy Requirements refer to ADDENDUM A and ADDENDUM B.

ADDENDUM A

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations.¹ The Contractor's firewall and web server shall meet or exceed the VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Each documented initiative under this contract incorporates the security clause VAAR 852.273-75 by reference as though fully set forth therein, as well as the VA Handbook 6500.6, "Contract Security," March 12, 2010, in its entirety. Both the security clause VAAR 852.273-75 and the VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses identified on the current external VA training site, the Employee Education System (EES), and will be tracked therein. The EES may be accessed at <https://www.ees-learning.net/librix/loginhtml.asp?v=librix>. Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at <http://www.ea.oit.va.gov/index.asp> in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). The VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

A2.1. VA Internet and Intranet Standards:

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

¹ See VAAR 852.273-75 referenced *infra*.

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed and published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

Section 508 – Electronic and Information Technology (EIT) Standards:

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: <http://www.section508.gov> and <http://www.access-board.gov/sec508/standards.htm>. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

- x § 1194.21 Software applications and operating systems
- x § 1194.22 Web-based intranet and internet information and applications
- x § 1194.23 Telecommunications products
- x § 1194.24 Video and multimedia products
- x § 1194.25 Self contained, closed products
- x § 1194.26 Desktop and portable computers
- x § 1194.31 Functional Performance Criteria
- x § 1194.41 Information, Documentation, and Support

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

A4.0 Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. The VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. The VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage

during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of the VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of the VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA Contracting Officer.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.

6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by the VA.
7. Contractor must adhere to the following:
8. The use of "thumb drives" or any other medium for transport of information is expressly prohibited.
9. Controlled access to system and security software and documentation.
10. Recording, monitoring, and control of passwords and privileges.
11. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
12. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
13. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
14. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
15. Contractor does not require access to classified data.
16. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.

ADDENDUM B

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010

B1. GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

1. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or Delivery Order.
2. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.
3. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.
4. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.
5. The Contractor or Subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The Contracting Officer must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in

- Rights in Data - General, FAR 52.227-14(d) (1).
2. VA information should not be co-mingled, if possible, with any other data on the Contractor/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.
 3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.
 4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.
 5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.
 6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.
 7. If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.
 8. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.
 9. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.
 10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of

- competent jurisdiction, or (ii) with VA's prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.
11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.
 12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an MOU-ISA for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COTR.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, *VA Information Security Program*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COTR, and approved by the VA Privacy Service in accordance with Directive 6507, *VA Privacy Impact Assessment*.
2. The Contractor/Subcontractor shall certify to the COTR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or the VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.
3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default "program files" directory and silently install and uninstall.
4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.
5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.
6. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.
7. The Contractor/Subcontractor agrees to:

- a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:
 - i. The Systems of Records (SOR); and
 - ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;
 - b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and
 - c. Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR
 8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.
 - a. "Operation of a System of Records" means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.
 - b. "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person's name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.
 - c. "System of Records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
 9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.
 10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, based upon the severity of the incident.
 11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to the VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within their contract.

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the contracting officer and the VA Assistant Secretary for Office of Information and Technology.

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

1. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COTR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's network involving VA information must be reviewed and approved by VA prior to implementation.
2. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.
3. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the Contractor's systems in accordance with VA Handbook 6500.3, *Certification and Accreditation* and/or the VA OCS Certification Program Office. Government-owned (government facility or government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.
4. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into VA's POA&M management process. The Contractor/Subcontractor must use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

5. The Contractor/Subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COTR. The government reserves the right to conduct such an assessment using government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.
6. VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on VA's network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.
7. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.
8. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:
 - a. Vendor must accept the system without the drive;
 - b. VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
 - c. VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
 - d. Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for the VA to retain the hard drive, then;
 - i. The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and
 - ii. Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.
 - iii. A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and

completed. The ISO needs to maintain the documentation.

B6. SECURITY INCIDENT INVESTIGATION

1. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COTR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.
2. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.
3. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.
4. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

1. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract.
2. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and

grounds for contract termination.

3. Each risk analysis shall address all relevant information concerning the data breach, including the following:
 - a. Nature of the event (loss, theft, unauthorized access);
 - b. Description of the event, including:
 - i. date of occurrence;
 - ii. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
 - c. Number of individuals affected or potentially affected;
 - d. Names of individuals or groups affected or potentially affected;
 - e. Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
 - f. Amount of time the data has been out of VA control;
 - g. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
 - h. Known misuses of data containing sensitive personal information, if any;
 - i. Assessment of the potential harm to the affected individuals;
 - j. Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
 - k. Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.
4. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to the VA liquidated damages in the amount of \$37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
 - a. Notification;
 - b. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
 - c. Data breach analysis;
 - d. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
 - e. One year of identity theft insurance with \$20,000.00 coverage at \$0 deductible; and
 - f. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B8. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the government, the Contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

B9. TRAINING

1. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
 - a. Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems;
 - b. Successfully complete the *VA Cyber Security Awareness and Rules of Behavior* training and annually complete required security training;
 - c. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
 - d. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access
2. The Contractor shall provide to the contracting officer and/or the COTR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.
3. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

SECTION D - PACKAGING AND MARKING

D.1 PACKAGING, HANDLING, STORAGE AND TRANSPORTATION

Packaging, Handling, Storage and Transportation requirements are outlined in the Commodities Enterprise Contract Performance Work Statement, Paragraph 11.0.

SECTION E - INSPECTION AND ACCEPTANCE

E.1	52.246-2	INSPECTION OF SUPPLIES--FIXED-PRICE	AUG 1996
E.2	52.246-4	INSPECTION OF SERVICES--FIXED-PRICE	AUG 1996
E.3	52.246-6	INSPECTION--TIME-AND-MATERIALS AND LABOR-HOUR	MAY 2001
E.4	52.246-16	RESPONSIBILITY FOR SUPPLIES	APR 1984
E.5	852.246-71	INSPECTION	JAN 2008

E.6 VAAR 852.246-70 GUARANTEE (JAN 2008)

The contractor guarantees the equipment against defective material, workmanship and performance for a period of one year, said guarantee to run from date of acceptance of the equipment by the Government. The contractor agrees to furnish, without cost to the Government, replacement of all parts and material that are found to be defective during the guarantee period. Replacement of material and parts will be furnished to the Government at the point of installation, if installation is within the continental United States, or f.o.b. the continental U.S. port to be designated by the contracting officer if installation is outside of the continental United States. Cost of installation of replacement material and parts shall be borne by the contractor.

(End of Clause)

SECTION F - DELIVERIES OR PERFORMANCE

F.1 52.242-15 STOP-WORK ORDER

AUG 1989

F.2 52.242-17 GOVERNMENT DELAY OF WORK

APR 1984

F.3 52.247-34 F.O.B. DESTINATION

NOV 1991

SECTION G - CONTRACT ADMINISTRATION DATA

G.1 CONTRACT ADMINISTRATION RESPONSIBILITIES

The Contract-level Contracting Officer (CO) is responsible for overall management and administration, the final close out of the contract, and as appropriate shall:

- 1) Provide contract scope oversight;
- 2) Serve as a liaison between the Contractor and VA;
- 3) Ensure compliance with contract requirements;
- 4) Issue CO final decisions with respect to contract-level disputes under the Disputes Clause of the Contract;
- 5) Issue all modifications against the Contract, including, but not limited to any change order modifications related to the Technology Refresh and Technology Insertion requirements of the Performance Work Statement.

The Delivery Order CO is responsible for preparing the Delivery Order Request for Proposals. In no event will a Delivery Order change the requirements of any CEC contracts. Should a contract user require a change, specific approval shall be obtained from the Contract-level CO. The Delivery Order CO is responsible for:

- 1) Issuing delivery orders consistent with the terms and conditions of the CEC Contract(s);
- 2) Completing any or all administrative contractual actions concerning individual delivery orders;
- 3) Terminating delivery orders, for convenience or default;
- 4) Ensuring that proposed delivery orders are within the scope of the Contract;
- 5) Ensuring inspection, acceptance and rejection of supplies or services;
- 6) Managing contractor invoices and ensuring timely payment;
- 7) Completing Contractor Performance Assessment Reports (CPARS) as appropriate; and
- 8) Administration and final closeout of delivery orders.

G.2 DELIVERY ORDER SOLICITATION

The Delivery Order CO shall ensure that a solicitation allows for a fair opportunity competition among all CEC contract holders, unless an exception to fair opportunity applies and is approved in accordance with Federal Acquisition Regulation (FAR) Subpart 16.505. The Solicitation may be processed manually or via an electronic process, if available. If available, solicitations may be issued using reverse auction applications. At a minimum, the Solicitation shall specify the Government's specific CEC IT Hardware Commodity Product, Warranty, Installation and/or Incidental Technical Support Services, delivery or period of performance requirements, and the due date for submission of proposals. The Request for Proposals shall also include specific instructions for proposal submissions. The Delivery Order CO shall determine the appropriate amount of time for proposal submission based upon the estimated value and complexity of the proposed delivery order requirements. The Solicitation shall specify the applicable Basis of Award for each Delivery Order as well as the applicable evaluation factors and sub-factors and their relative order of importance.

G.3 DELIVERY ORDER PROCEDURES

The Delivery Order CO shall provide fair opportunity to each CEC Contractor to be considered for all Delivery Orders exceeding the micro-purchase threshold (\$3,000), unless an exception to fair opportunity

under FAR Subpart 16.505(b)(2) applies. Electronic ordering capability, if available, shall be used to the maximum extent practicable. If an electronic process is not available, a manual solicitation process (e-mail) shall be used. The Government expects all contractors to submit a proposal on all future delivery order solicitations. By submitting a proposal for award of a CEC IDIQ contract, the Contractor is confirming its intention to compete for all future delivery orders, unless unable to compete. The parties agree that this is a material clause of the Contract.

If the Contractor intends not to submit a proposal, the contractor must notify the delivery order CO of that intent in advance of the closing date of the delivery order solicitation, for CO approval. Such notifications must show cause why the company is unable to compete, and demonstrate in detail why it has an inability to compete.

Failure to comply with this material clause may result in the Government pursuing any and all remedies set forth in this Contract, including, but not limited to Termination for Default.

The CEC Contractor's proposal shall address all aspects of the proposal submission instructions set forth in the Delivery Order Solicitation, including, but not limited to:

- 1) Proposed IT Hardware Commodity Product (OEM part number);
- 2) Proposed Extended Warranty and Installation Support (if applicable);
- 3) Proposed Incidental Technical Support Services including proposed subcontractors (if applicable);
- 4) Delivery terms; and
- 5) Other pertinent data.

The proposal shall include detailed firm fixed prices for all products, warranty and standard installation support required. The proposal shall include detailed T&M pricing including applicable travel and other direct costs/material. The Contractor may propose firm fixed prices, loaded hourly T&M rates and applicable T&M material handling fees less than what is specified in the Contract; however, contract awardees may not propose firm fixed prices, loaded hourly T&M rates, or applicable T&M material handling fees that exceed those set forth in their respective CEC Contract. The Government shall not reimburse CEC Contractors for direct charges associated with the preparation and/or submission of proposals.

G.4 DELIVERY ORDER CONTENTS AND ISSUANCE

Delivery Orders issued under this Contract shall contain the following information:

- 1) Date of order;
- 2) Contract and order number;
- 3) Contract item number, description, quantity, unit and extended prices as appropriate;
- 4) Delivery schedule and/or period of performance;
- 5) Delivery location and/or place of performance;
- 6) Packaging, packing or shipping instructions;
- 7) Accounting and appropriation data, as well as Integrated Funds Distribution, Control Point Activity, Accounting and Procurement (IFCAP) purchase order number for VA orders; and
- 8) Method for submitting invoices, method of payment, and payment office.

Delivery Orders shall be issued on Optional Form 347 (or agency prescribed form) to the selected CEC Contractor. Under no circumstances shall the Contractor commence performance before issuance of a signed Delivery Order or other written approval by the Delivery Order CO or the Contract level CO.

G.5 FAIR OPPORTUNITY

In accordance with the ordering provisions of FAR Subpart 16.505(b)(1), Delivery Order COs shall provide proposed Delivery Order solicitations, either manually or by electronic process if available, to each CEC awardee so to provide a fair opportunity to be considered for each Delivery Order award. Fair opportunity need not be provided if the following applies:

- 1) If the total value of a proposed delivery order is less than the micro-purchase threshold (\$3,000), the Delivery Order CO may make an award without seeking competitive proposals based upon existing pricing in a CEC contract; or
- 2) One of the exceptions to fair opportunity as specified at FAR Subpart 16.505(b)(2) applies and the required justification is approved and published consistent with this subpart.

G.6 INVOICING AND PAYMENT

Individual Delivery Orders shall specify the applicable instructions for submission of invoices to the designated Payment Offices. Invoices for Delivery Orders including time and material line items shall be billed and processed in accordance with FAR 52.232-7, Payments under Time-and-Materials and Labor-Hour Contracts (Feb 2007).

G.7 LIMITATIONS ON SUBCONTRACTING – MONITORING AND COMPLIANCE

This Contract includes FAR 52.219-6, Notice of Total Small Business Set-Aside and FAR 52.219-14, Limitations on Subcontracting. The Contractor is advised that in performing contract administration functions, the CO may use the services of a support contractor(s) retained by VA to assist in assessing the Contractor's compliance with the limitations on subcontracting or percentage of work performance requirements specified in the clause. To that end, the support contractor(s) may require access to the Contractor's offices where the Contractor's business records or other proprietary data are retained and to review such business records regarding the Contractor's compliance with this requirement. All support contractors conducting this review on behalf of VA will be required to sign an "Information Protection and Non-Disclosure and Disclosure of Conflicts of Interest Agreement" to ensure the Contractor's business records or other proprietary data reviewed or obtained in the course of assisting the CO in assessing the Contractor for compliance are protected to ensure information or data is not improperly disclosed or other impropriety occurs. Furthermore, if VA determines any services the support contractor(s) will perform in assessing compliance are advisory and assistance services as defined in FAR 2.101, Definitions, the support contractor(s) must also enter into an agreement with the Contractor to protect proprietary information as required by FAR 9.505-4, Obtaining access to proprietary information, paragraph (b). The Contractor is required to cooperate fully and make available any records as may be required to enable the CO to assess the Contractor's compliance with the limitations on subcontracting or percentage of work performance requirement.

SECTION H - SPECIAL CONTRACT REQUIREMENTS

H.1 TERM OF CONTRACT

The term of the Commodities Enterprise Contract (CEC) shall provide for placement of orders for a period of five (5) years from date of contract award in accordance with applicable Firm Fixed Price (FFP) and Time and Materials (T&M) line items for each ordering year set forth in the Contract Schedule B. Extended Standard or Premium Warranties may be acquired as options under delivery orders placed prior to expiration of the five (5) year ordering period. Performance of each Delivery Order awarded prior to Contract expiration may require continued warranty technical support services as described in Section 9.0 of the Performance Work Statement for a maximum of five (5) years after the expiration of the five (5) year ordering period.

H.2 CONTRACT TOTAL MINIMUM AND MAXIMUM QUANTITIES

In accordance with Federal Acquisition Regulation (FAR) 52.216-22, "Indefinite Quantity," the minimum quantity of supplies/services the Government shall acquire under any resulting individual CEC contract is for an amount of at least \$150,000.00. The cumulative value of all Task Orders issued under the CEC Program shall not exceed \$5,314,335,810.00.

H.3 AGENCY DELIVERY ORDER OMBUDSMAN

The Agency Delivery Order Ombudsman shall review any complaints from contractors to ensure they are afforded a fair opportunity to be considered, consistent with the procedures specified in the resulting contract. The Department of Veterans Affairs Delivery Order Ombudsman and associated contact information is as follows:

Mr. C. Ford Heard III
Associate Deputy Assistant Secretary for Procurement, Policy, Systems and Oversight (003A2)
810 Vermont Ave., NW
Washington, DC 20402
(202) 461-6821
Ford.Heard@va.gov

H.4 ACTIVITIES AUTHORIZED TO ISSUE ORDERS

At this time, only appointed Contracting Officers within the VA Technology Acquisition Center (TAC) shall be authorized to issue orders under any resulting CEC contracts. Although the primary objective of this acquisition is to establish a Commodities Enterprise arrangement that will ensure standardization of commercial Information Technology (IT) hardware and associated installation, configuration, warranty, maintenance and technical support services solutions across the VA Enterprise in support of the VA Office of Information and Technology (OIT), the TAC may also issue orders for requirements within the scope of the CEC contracts from other Federal agency customers. Any requirements from other Federal Agency customers outside of VA shall be approved through Inter-agency Agreements to provide assisted acquisition support through the CEC contracts. The Government reserves the right to subsequently authorize other Contracting Officers within VA to issue orders. Oral orders shall not be authorized for placement under any resulting CEC contracts.

H.5 CEC IT HARDWARE COMMODITY CEILING PRICES

The Contractor's Price List incorporated into this Contract serves as the basis for prices for the IT Hardware Commodity products, warranties and installation for each of the ordering years specified in the Contract Schedule in Section B. These prices are binding on all awardees for each of the applicable ordering years, regardless of the quantity being ordered. With respect to Networking Appliances, Contractor's are hereby advised that the price proposed for the specific configuration incorporated by Attachment No. 009 shall serve as the ceiling price for any and all variants. Consistent with the Technology Refresh requirements of the CEC PWS and Attachment A thereto, the Contractor cannot submit an ECP for Technology Refresh of an IT Hardware Commodity Product that reflects a price higher than that proposed in Section J, Attachment No. 009, and incorporated into the Contract.

H.6 CEC INCIDENTAL TECHNICAL SUPPORT SERVICES CEILING PRICE

Attachment No. 010 ("T&M Labor Rates"), which is incorporated into this Contract, establishes the Contractor's and proposed Subcontractor's loaded hourly T&M rates for each of the ordering periods specified in both the Contract Schedule in Section B, and Section H-7 below. These loaded hourly T&M rates reflect the maximum rates that the Contractor can propose for a Delivery Order issued in a given ordering period, for both its self as prime contractor and any of its subcontractors.

H-7 ORDERING PERIODS

There are five (5) one(1)-year Ordering Periods associated with this Contract for which corresponding pricing is established. The periods of performance for the five (5) one (1)-year Ordering Periods are as follows:

1. Ordering Period 1 will begin at contract award and end on the 365th day after contract award.
2. Ordering Period 2 will begin on the 366th day after award and end on the 731st day after contract award.
3. Ordering Period 3 will begin on the 732nd day after contract award and end on the 1,097th day after contract award.
4. Ordering Period 4 will begin on the 1098th day after contract award and end on the 1,463th day after contract award.
5. Ordering Period 5 will begin on the 1,464th day after contract award and end on the 1,828th day after contract award.

H-8 ON-RAMP/OFF-RAMP

In accordance with the Solicitation, CEC has been established as a competitive Total Small Business Set-Aside, with one (1) award specifically reserved for an SDVOSB concern. In order to facilitate adequate competition on all CEC delivery orders, and ensure that the size and status certification requirements of CEC contract holders are maintained throughout the period of performance established by Subsection H.1, the Government hereby reserves the right to utilize an ON-RAMP/OFF-RAMP approach, as described below, when necessary.

H-8.1 OFF-RAMP

In the event that a CEC contract holder is acquired by an other than Small Business concern; an SDVOSB for which an award was reserved no longer qualifies as an SDVOSB concern; and/or an SDVOSB contract holder is acquired by a non-SDVOSB concern, the Government may "OFF-RAMP," or remove, the Contractor from the Contract via any remedies permissible under the Contract, at no cost to the

Government. As a result, the Contractor shall have no further rights under the Contract and thus, will not be eligible to propose on any CEC delivery order competitions, once removed.

H-8.2 ON-RAMP

If an OFF-RAMP is exercised, the Government may utilize an ON-RAMP to add Small Business or SDVOSB Prime Contractors to replace those removed via the OFF-RAMP process. At all times the Government shall ensure that, in accordance with the Solicitation, no more than three (3) awards are maintained, and that one (1) of those awards is reserved for an SDVOSB concern, to the greatest extent possible. In its sole discretion, the Government shall ON-RAMP any and all contractors by any means necessary, including but not limited to, revisiting the original pool of CEC Offerors deemed in the competitive range, and/or issuing a new solicitation for evaluation. Any contract awarded via the ON-RAMP process will share in, and in no way increase, the ceiling established for the CEC program. Likewise, contracts awarded hereunder shall include the same terms and conditions of this Contract and shall not exceed the remaining period of performance.

PART II - CONTRACT CLAUSES**SECTION I - CONTRACT CLAUSES****I.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)**

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

<http://www.acquisition.gov/far/index.html>

<http://www.va.gov/oamm/oa/ars/policyreg/vaar/index.cfm>

52.202-1	DEFINITIONS	JUL 2004
52.203-3	GRATUITIES	APR 1984
52.203-5	COVENANT AGAINST CONTINGENT FEES	APR 1984
52.203-6	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT	SEP 2006
52.203-7	ANTI-KICKBACK PROCEDURES	OCT 2010
52.203-8	CANCELLATION, RESCISSION, AND RECOVERY OF FUNDS FOR ILLEGAL OR IMPROPER ACTIVITY	JAN 1997
52.203-10	PRICE OR FEE ADJUSTMENT FOR ILLEGAL OR IMPROPER ACTIVITY	JAN 1997
52.203-12	LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS	OCT 2010
52.203-13	CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT	APR 2010
52.204-4	PRINTED OR COPIED DOUBLE-SIDED ON RECYCLED PAPER	MAY 2011
52.204-7	CENTRAL CONTRACTOR REGISTRATION	APR 2008
52.204-10	REPORTING EXECUTIVE COMPENSATION AND FIRST-TIER SUBCONTRACT AWARDS	JUL 2010
52.209-6	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT	DEC 2010
52.210-1	MARKET RESEARCH	APR 2011
52.211-5	MATERIAL REQUIREMENTS	AUG 2000
52.215-2	AUDIT AND RECORDS--NEGOTIATION	OCT 2010
52.215-8	ORDER OF PRECEDENCE--UNIFORM CONTRACT FORMAT	OCT 1997
52.215-10	PRICE REDUCTION FOR DEFECTIVE CERTIFIED COST OR PRICING DATA	AUG 2011
52.215-11	PRICE REDUCTION FOR DEFECTIVE CERTIFIED	AUG 2011

52.215-12	COST OR PRICING DATA – MODIFICATIONS SUBCONTRACTOR CERTIFIED COST OR PRICING DATA	OCT 2010
52.215-13	SUBCONTRACTOR CERTIFIED COST OR PRICING DATA - MODIFICATIONS	OCT 2010
52.215-14	INTEGRITY OF UNIT PRICES	OCT 2010
52.215-15	PENSION ADJUSTMENT AND ASSET REVERSIONS	OCT 2010
52.215-16	FACILITIES CAPITAL COST OF MONEY	JUN 2001
52.215-17	WAIVER OF FACILITIES CAPITAL COST OF MONEY	OCT 1997
52.215-18	REVERSION OR ADJUSTMENT OF PLANS FOR POSTRETIREMENT BENEFITS (PRB) OTHER THAN PENSIONS	JUL 2005
52.215-19	NOTIFICATION OF OWNERSHIP CHANGES	OCT 1997
52.216-7	ALLOWABLE COST AND PAYMENT	JUN 2011
52.217-7	OPTION FOR INCREASED QUANTITY – SEPARATELY PRICED LINE ITEM	MAR 1989
52.219-6	NOTICE OF TOTAL SMALL BUSINESS SET-ASIDE	JUN 2003
52.219-8	UTILIZATION OF SMALL BUSINESS CONCERNS	JAN 2011
52.219-14	LIMITATIONS ON SUBCONTRACTING	DEC 1996
52.222-3	CONVICT LABOR	JUN 2003
52.222-19	CHILD LABOR - COOPERATION WITH AUTHORITIES AND REMEDIES	JUL 2010
52.222-20	WALSH-HEALEY PUBLIC CONTRACTS ACT	OCT 2010
52.222-21	PROHIBITION OF SEGREGATED FACILITIES	FEB 1999
52.222-26	EQUAL OPPORTUNITY	MAR 2007
52.222-29	NOTIFICATION OF VISA DENIAL	JUN 2003
52.222-35	EQUAL OPPORTUNITY FOR VETERANS	SEP 2010
52.222-36	AFFIRMATIVE ACTION FOR WORKERS WITH DISABILITIES	OCT 2010
52.222-37	EMPLOYMENT REPORTS ON VETERANS	SEP 2010
52.222-41	SERVICE CONTRACT ACT OF 1965	NOV 2007
52.222-42	STATEMENT OF EQUIVALENT RATES FOR FEDERAL HIRES	MAY 1989
52.222-43	FAIR LABOR STANDARDS ACT AND SERVICE CONTRACT ACT-PRICE ADJUSTMENT (MULTIPLE YEAR AND OPTION CONTRACTS)	SEP 2009
52.222-50	COMBATING TRAFFICKING IN PERSONS	FEB 2009
52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION	JAN 2009
52.223-5	POLLUTION PREVENTION AND RIGHT-TO-KNOW INFORMATION	MAY 2011
52.223-15	ENERGY EFFICIENCY IN ENERGY-CONSUMING PRODUCTS	DEC 2007
52.223-16	IEEE 1680 STANDARD FOR THE ENVIRONMENTAL ASSESSMENT OF PERSONAL COMPUTER PRODUCTS	DEC 2007
52.223-18	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING	AUG 2011
52.225-13	RESTRICTIONS ON CERTAIN FOREIGN PURCHASES	JUN 2008
52.227-1	AUTHORIZATION AND CONSENT	DEC 2007
52.227-2	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT	DEC 2007

52.227-14	RIGHTS IN DATA--GENERAL	DEC 2007
52.227-19	COMMERCIAL COMPUTER SOFTWARE LICENSE	DEC 2007
52.228-5	INSURANCE--WORK ON A GOVERNMENT INSTALLATION	JAN 1997
52.229-3	FEDERAL, STATE, AND LOCAL TAXES	APR 2003
52.223-6	DRUG-FREE WORKPLACE	MAY 2001
52.232-1	PAYMENTS	APR 1984
52.232-7	PAYMENTS UNDER TIME-AND-MATERIALS AND LABOR-HOUR CONTRACTS	FEB 2007
52.232-8	DISCOUNTS FOR PROMPT PAYMENT	FEB 2002
52.232-11	EXTRAS	APR 1984
52.232-17	INTEREST	OCT 2010
52.232-23	ASSIGNMENT OF CLAIMS	JAN 1986
52.232-25	PROMPT PAYMENT	OCT 2008
52.232-33	PAYMENT BY ELECTRONIC FUNDS--CENTRAL CONTRACTOR REGISTRATION	OCT 2003
52.233-1	DISPUTES	JUL 2002
52.233-3	PROTEST AFTER AWARD	AUG 1996
52.233-4	APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM	OCT 2004
52.237-10	IDENTIFICATION OF UNCOMPENSATED OVERTIME	OCT 1997
52.237-2	PROTECTION OF GOVERNMENT BUILDINGS, EQUIPMENT, AND VEGETATION	APR 1984
52.237-3	CONTINUITY OF SERVICES	JAN 1991
52.239-1	PRIVACY OR SECURITY SAFEGUARDS	AUG 1996
52.242-13	BANKRUPTCY	JUL 1995
52.243-1	CHANGES--FIXED-PRICE	AUG 1987
52.243-3	CHANGES--TIME-AND-MATERIALS OR LABOR-HOURS	SEP 2000
52.244-2	SUBCONTRACTS	OCT 2010
52.244-5	COMPETITION IN SUBCONTRACTING	DEC 1996
52.244-6	SUBCONTRACTS FOR COMMERCIAL ITEMS	DEC 2010
52.245-1	GOVERNMENT PROPERTY	AUG 2010
52.245-9	USE AND CHARGES	AUG 2010
52.246-23	LIMITATION OF LIABILITY	FEB 1997
52.246-25	LIMITATION OF LIABILITY--SERVICES	FEB 1997
52.247-63	PREFERENCE FOR U.S.-FLAG AIR CARRIERS	JUN 2003
52.249-2	TERMINATION FOR CONVENIENCE OF THE GOVERNMENT (FIXED-PRICE)	MAY 2004
52.249-6	TERMINATION (COST-REIMBURSEMENT) ALTERNATE IV (SEP 1996)	SEP 1996
52.249-8	DEFAULT (FIXED-PRICE SUPPLY AND SERVICE)	APR 1984
52.249-14	EXCUSABLE DELAYS	APR 1984
52.253-1	COMPUTER GENERATED FORMS	JAN 1991
852.203-70	COMMERCIAL ADVERTISING	JAN 2008
852.203-71	DISPLAY OF DEPARTMENT OF VETERANS AFFAIRS HOTLINE POSTER	DEC 1992

I.2 52.209-9 UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS (JAN 2011)

(a) The Contractor shall update the information in the Federal Awardee Performance and Integrity Information System (FAPIIS) on a semi-annual basis, throughout the life of the contract, by posting the required information in the Central Contractor Registration database at <http://www.ccr.gov>.

(b)(1) The Contractor will receive notification when the Government posts new information to the Contractor's record.

(2) The Contractor will have an opportunity to post comments regarding information that has been posted by the Government. The comments will be retained as long as the associated information is retained, i.e., for a total period of 6 years. Contractor comments will remain a part of the record unless the Contractor revises them.

(3)(i) Public requests for system information posted prior to April 15, 2011, will be handled under Freedom of Information Act procedures, including, where appropriate, procedures promulgated under E.O. 12600.

(ii) As required by section 3010 of Public Law 111-212, all information posted in FAPIIS on or after April 15, 2011, except past performance reviews, will be publicly available.

(End of Clause)

I.3 52.216-18 ORDERING (OCT 1995)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from the date of contract award through 60 months after the date of contract award.

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c) If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

(End of Clause)

I.4 52.216-19 ORDER LIMITATIONS (OCT 1995)

(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than \$3,000.00, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) Maximum order. The Contractor is not obligated to honor--

(1) Any order for a single item in excess of \$100,000,000.00;

(2) Any order for a combination of items in excess of \$100,000,000.00; or

(3) A series of orders from the same ordering office within 30 days that together call for quantities exceeding the limitation in paragraph (b)(1) or (2) of this section.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within 5 days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of Clause)

I.5 52.216-22 INDEFINITE QUANTITY (OCT 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after 60 months after the expiration date of the basic contract.

(End of Clause)

I-6 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of the contract by written notice to the Contractor within 30 days from expiration of the contract; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

- (c) The total duration of this contract, including the exercise of any options under this clause shall not exceed 10 years from date of award.

(End of Clause)

I.7 52.219-28 POST-AWARD SMALL BUSINESS PROGRAM REREPRESENTATION (APR 2009)

- (a) Definitions. As used in this clause-

Long-term contract means a contract of more than five years in duration, including options. However, the term does not include contracts that exceed five years in duration because the period of performance has been extended for a cumulative period not to exceed six months under the clause at 52.217-8, Option to Extend Services, or other appropriate authority.

Small business concern means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR part 121 and the size standard in paragraph (c) of this clause. Such a concern is "not dominant in its field of operation" when it does not exercise a controlling or major influence on a national basis in a kind of business activity in which a number of business concerns are primarily engaged. In determining whether dominance exists, consideration shall be given to all appropriate factors, including volume of business, number of employees, financial resources, competitive status or position, ownership or control of materials, processes, patents, license agreements, facilities, sales territory, and nature of business activity.

- (b) If the Contractor represented that it was a small business concern prior to award of this contract, the Contractor shall rerepresent its size status according to paragraph (e) of this clause or, if applicable, paragraph (g) of this clause, upon the occurrence of any of the following:

(1) Within 30 days after execution of a novation agreement or within 30 days after modification of the contract to include this clause, if the novation agreement was executed prior to inclusion of this clause in the contract.

(2) Within 30 days after a merger or acquisition that does not require a novation or within 30 days after modification of the contract to include this clause, if the merger or acquisition occurred prior to inclusion of this clause in the contract.

- (3) For long-term contracts-

(i) Within 60 to 120 days prior to the end of the fifth year of the contract; and

(ii) Within 60 to 120 days prior to the date specified in the contract for exercising any option thereafter.

(c) The Contractor shall rerepresent its size status in accordance with the size standard in effect at the time of this rerepresentation that corresponds to the North American Industry Classification System (NAICS) code assigned to this contract. The small business size standard corresponding to this NAICS code can be found at <http://www.sba.gov/services/contractingopportunities/sizestandardstopics/>.

(d) The small business size standard for a Contractor providing a product which it does not manufacture itself, for a contract other than a construction or service contract, is 500 employees.

(e) Except as provided in paragraph (g) of this clause, the Contractor shall make the rerepresentation required by paragraph (b) of this clause by validating or updating all its representations in the Online Representations and Certifications Application and its data in the Central Contractor Registration, as necessary, to ensure that they reflect the Contractor's current status. The Contractor shall notify the contracting office in writing within the timeframes specified in paragraph (b) of this clause that the data have been validated or updated, and provide the date of the validation or update.

(f) If the Contractor represented that it was other than a small business concern prior to award of this contract, the Contractor may, but is not required to, take the actions required by paragraphs (e) or (g) of this clause.

(g) If the Contractor does not have representations and certifications in ORCA, or does not have a representation in ORCA for the NAICS code applicable to this contract, the Contractor is required to complete the following rerepresentation and submit it to the contracting office, along with the contract number and the date on which the rerepresentation was completed:

The Contractor represents that it [] is, [] is not a small business concern under NAICS Code 541519 IT VAR exception, for which the small business size standard is 150 employees.

[Contractor to sign and date and insert authorized signer's name and title].

(End of Clause)

I.8 52.222-40 NOTIFICATION OF EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT (DEC 2010)

(a) During the term of this contract, the Contractor shall post an employee notice, of such size and in such form, and containing such content as prescribed by the Secretary of Labor, in conspicuous places in and about its plants and offices where employees covered by the National Labor Relations Act engage in activities relating to the performance of the contract, including all places where notices to employees are customarily posted both physically and electronically, in the languages employees speak, in accordance with 29 CFR 471.2(d) and (f).

(1) Physical posting of the employee notice shall be in conspicuous places in and about the Contractor's plants and offices so that the notice is prominent and readily seen by employees who are covered by the National Labor Relations Act and engage in activities related to the performance of the contract.

(2) If the Contractor customarily posts notices to employees electronically, then the Contractor shall also post the required notice electronically by displaying prominently, on any Web site that is maintained by the Contractor and is customarily used for notices to employees about terms and conditions of employment, a link to the Department of Labor's Web site that contains the full text of the poster. The link to the Department's Web site, as referenced in (b)(3) of this section, must read, "Important Notice about Employee Rights to Organize and Bargain Collectively with Their Employers."

(b) This required employee notice, printed by the Department of Labor, may be-

(1) Obtained from the Division of Interpretations and Standards, Office of Labor-Management Standards, U.S. Department of Labor, 200 Constitution Avenue, NW., Room N-5609, Washington, DC 20210, (202) 693-0123, or from any field office of the Office of Labor-Management Standards or Office of Federal Contract Compliance Programs;

(2) Provided by the Federal contracting agency if requested;

(3) Downloaded from the Office of Labor-Management Standards Web site at <http://www.dol.gov/olms/regs/compliance/EO13496.htm>; or

(4) Reproduced and used as exact duplicate copies of the Department of Labor's official poster.

(c) The required text of the employee notice referred to in this clause is located at Appendix A, Subpart A, 29 CFR Part 471.

(d) The Contractor shall comply with all provisions of the employee notice and related rules, regulations, and orders of the Secretary of Labor.

(e) In the event that the Contractor does not comply with the requirements set forth in paragraphs (a) through (d) of this clause, this contract may be terminated or suspended in whole or in part, and the Contractor may be suspended or debarred in accordance with 29 CFR 471.14 and subpart 9.4. Such other sanctions or remedies may be imposed as are provided by 29 CFR part 471, which implements Executive Order 13496 or as otherwise provided by law.

(f) Subcontracts.

(1) The Contractor shall include the substance of this clause, including this paragraph (f), in every subcontract that exceeds \$10,000 and will be performed wholly or partially in the United States, unless exempted by the rules, regulations, or orders of the Secretary of Labor issued pursuant to section 3 of Executive Order 13496 of January 30, 2009, so that such provisions will be binding upon each subcontractor.

(2) The Contractor shall not procure supplies or services in a way designed to avoid the applicability of Executive Order 13496 or this clause.

(3) The Contractor shall take such action with respect to any such subcontract as may be directed by the Secretary of Labor as a means of enforcing such provisions, including the imposition of sanctions for noncompliance.

(4) However, if the Contractor becomes involved in litigation with a subcontractor, or is threatened with such involvement, as a result of such direction, the Contractor may request the United States, through the Secretary of Labor, to enter into such litigation to protect the interests of the United States.

(End of Clause)

I.9 52.227-3 PATENT INDEMNITY (APR 1984)

(a) The Contractor shall indemnify the Government and its officers, agents, and employees against liability, including costs, for infringement of any United States patent (except a patent issued upon an application that is now or may hereafter be withheld from issue pursuant to a Secrecy Order under 35

U.S.C. 181) arising out of the manufacture or delivery of supplies, the performance of services, or the construction, alteration, modification, or repair of real property (hereinafter referred to as "construction work") under this contract, or out of the use or disposal by or for the account of the Government of such supplies or construction work.

(b) This indemnity shall not apply unless the Contractor shall have been informed as soon as practicable by the Government of the suit or action alleging such infringement and shall have been given such opportunity as is afforded by applicable laws, rules, or regulations to participate in its defense. Further, this indemnity shall not apply to (1) an infringement resulting from compliance with specific written instructions of the Contracting Officer directing a change in the supplies to be delivered or in the materials or equipment to be used, or directing a manner of performance of the contract not normally used by the Contractor, (2) an infringement resulting from addition to or change in supplies or components furnished or construction work performed that was made subsequent to delivery or performance, or (3) a claimed infringement that is unreasonably settled without the consent of the Contractor, unless required by final decree of a court of competent jurisdiction.

(End of Clause)

I.10 52.246-20 WARRANTY OF SERVICES (MAY 2001)

(a) Definition. "Acceptance," as used in this clause, means the act of an authorized representative of the Government by which the Government assumes for itself, or as an agent of another, ownership of existing and identified supplies, or approves specific services, as partial or complete performance of the contract.

(b) Notwithstanding inspection and acceptance by the Government or any provision concerning the conclusiveness thereof, the Contractor warrants that all services performed under this contract will, at the time of acceptance, be free from defects in workmanship and conform to the requirements of this contract. The Contracting Officer shall give written notice of any defect or nonconformance to the Contractor within 30 days from the date of acceptance by the Government. This notice shall state either (1) that the Contractor shall correct or reperform any defective or nonconforming services, or (2) that the Government does not require correction or reperformance.

(c) If the Contractor is required to correct or reperform, it shall be at no cost to the Government, and any services corrected or reperformed by the Contractor shall be subject to this clause to the same extent as work initially performed. If the Contractor fails or refuses to correct or reperform, the Contracting Officer may, by contract or otherwise, correct or replace with similar services and charge to the Contractor the cost occasioned to the Government thereby, or make an equitable adjustment in the contract price.

(d) If the Government does not require correction or reperformance, the Contracting Officer shall make an equitable adjustment in the contract price.

(End of Clause)

I.11 852.211-75 PRODUCT SPECIFICATIONS (JAN 2008)

The products offered under this contract shall be in accordance with the specifications outlined in Attachment Nos. 2 through 8 outlined in Section J and all other requirements outlined herein.

(End of Clause)

I.12 VAAR 852.215-71 EVALUATION FACTOR COMMITMENTS (DEC 2009)

The offeror agrees, if awarded a contract, to use the service-disabled veteran-owned small businesses or veteran-owned small businesses proposed as subcontractors in accordance with 852.215-70, Service-Disabled Veteran-Owned and Veteran-Owned Small Business Evaluation Factors, or to substitute one or more service-disabled veteran-owned small businesses or veteran-owned small businesses for subcontract work of the same or similar value.

(End of Clause)

I.13 VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984)

The contractor shall obtain all necessary licenses and/or permits required to perform this work. He/she shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract. He/ she shall be responsible for any injury to himself/herself, his/her employees, as well as for any damage to personal or public property that occurs during the performance of this contract that is caused by his/her employees fault or negligence, and shall maintain personal liability and property damage insurance having coverage for a limit as required by the laws of the State of (TBD). Further, it is agreed that any negligence of the Government, its officers, agents, servants and employees, shall not be the responsibility of the contractor hereunder with the regard to any claims, loss, damage, injury, and liability resulting there from.

(End of Clause)

I.14 VAAR 852.270-1 REPRESENTATIVES OF CONTRACTING OFFICERS (JAN 2008)

The contracting officer reserves the right to designate representatives to act for him/her in furnishing technical guidance and advice or generally monitor the work to be performed under this contract. Such designation will be in writing and will define the scope and limitation of the designee's authority. A copy of the designation shall be furnished to the contractor.

(End of Provision)

I.15 VAAR 852.273-75 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (Interim - October 2008)

(a) The contractor and their personnel shall be subject to the same Federal laws, regulations, standards and VA policies as VA personnel, regarding information and information system security. These include, but are not limited to Federal Information Security Management Act (FISMA), Appendix III of OMB Circular A-130, and guidance and standards, available from the Department of Commerce's National Institute of Standards and Technology (NIST). This also includes the use of common security configurations available from NIST's Web site at:

<http://checklists.nist.gov>

(b) To ensure that appropriate security controls are in place, Contractors must follow the procedures set forth in "VA Information and Information System Security/Privacy Requirements for IT Contracts" located at the following Web site:

http://www.iprm.oit.va.gov/docs/Security_and_Privacy_Requirements_for_IT_Contracts_Attachment.pdf

(End of Clause)

I.16 VAAR 852.273-76 ELECTRONIC INVOICE SUBMISSION (Interim - October 2008)

(a) To improve the timeliness of payments and lower overall administrative costs, VA strongly encourages contractors to submit invoices using its electronic invoicing system. At present, electronic submission is voluntary and any nominal registration fees will be the responsibility of the contractor. VA intends to mandate electronic invoice submission, subject to completion of the federal rulemaking process. At present, VA is using a 3rd party agent to contact contractors regarding this service. During the voluntary period, contractors interested in registering for the electronic system should contact the VA's Financial Services Center at <http://www.fsc.va.gov/einvoice.asp>.

I.17 SUPPLEMENTAL INSURANCE REQUIREMENTS

In accordance with FAR 28.307-2 and FAR 52.228-5, the following minimum coverage shall apply to this contract:

(a) Workers' compensation and employers liability: Contractors are required to comply with applicable Federal and State workers' compensation and occupational disease statutes. If occupational diseases are not compensable under those statutes, they shall be covered under the employer's liability section of the insurance policy, except when contract operations are so commingled with a Contractor's commercial operations that it would not be practical to require this coverage. Employer's liability coverage of at least \$100,000 is required, except in States with exclusive or monopolistic funds that do not permit workers' compensation to be written by private carriers.

(b) General Liability: \$500,000.00 per occurrences.

(c) Automobile liability: \$200,000.00 per person; \$500,000.00 per occurrence and \$20,000.00 property damage.

(d) The successful bidder must present to the Contracting Officer, prior to award, evidence of general liability insurance without any exclusionary clauses for asbestos that would void the general liability coverage.

(End of Clause)

I.18 MANDATORY WRITTEN DISCLOSURES

Mandatory written disclosures required by FAR clause 52.203-13 to the Department of Veterans Affairs, Office of Inspector General (OIG) must be made electronically through the VA OIG Hotline at <http://www.va.gov/oig/contacts/hotline.asp> and clicking on "FAR clause 52.203-13 Reporting." If you experience difficulty accessing the website, call the Hotline at 1-800-488-8244 for further instructions.

PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

SECTION J - LIST OF ATTACHMENTS

ATTACHMENT NO. 001 – PWS Attachment A - Engineering Change Proposal
ATTACHMENT NO. 002 – PWS Attachment B - End User Device Specifications, Rev 5
ATTACHMENT NO. 003 – PWS Attachment C - Mobile Tablet Specifications, Rev 2
ATTACHMENT NO. 004 – PWS Attachment D - Server Specifications, Rev 2
ATTACHMENT NO. 005 – PWS Attachment E – Networking Appliances - Switch Specifications, Rev 1
ATTACHMENT NO. 006 – PWS Attachment F – Networking Appliances - Router Specifications, Rev 1
ATTACHMENT NO. 007 – PWS Attachment G –Storage Arrays/Storage Appliance Specifications, Rev 1
ATTACHMENT NO. 008 – PWS Attachment H – Security Platform Specifications, Rev 1
ATTACHMENT NO. 009 – Price.pdf (January 16, 2013)
ATTACHMENT NO. 010 – T&M Labor Rates
ATTACHMENT NO. 011 – Labor Category Descriptions (excel)
ATTACHMENT NO. 012 – PWS Attachment I - CEC Call Flow

Engineering Change Proposals (ECPs) for Technology Refresh and Technology Insertion

Technological changes over time in information technology (IT) products and hardware may result in the need to update the VA's CEC IT hardware commodity contract items under the applicable technical functional areas. To ensure that these changes are properly documented and managed, the Contractor shall submit a Configuration Management Plan for Government approval as a deliverable under the resulting Contract in accordance with PWS paragraph 5.1.7. As part of this Plan, the Contractor may be required, or elect, to submit Engineering Change Proposals (ECPs) for Technology Refresh with respect to replacement or updating of existing IT hardware commodity products (PWS paragraph 5.1.8) or Technology Insertion for new hardware products or technologies (PWS paragraph 5.1.9) deemed within the general scope of the Contract by the Contracting Officer (CO). ECPs, whether for Technology Refreshment or Technology Insertion, shall be submitted to the CO and Contracting Officer's Technical Representative (COTR). Approved ECPs that incorporate new or replacement IT hardware commodity products through Technology Refresh or Technology Insertion shall apply with respect to delivery orders subsequently issued under the contract. That is, the Contractor shall not be required to retrofit IT hardware commodity products previously delivered and/or installed under the contract, unless the proposed change corrects a problem or hazard with the existing installed hardware. The Government shall have the right to acquire, at any time, state of the art IT hardware commodity products as defined by the Technical Functional Areas in PWS paragraphs 6.0 through 6.6 available to the Contractor's commercial customers. Under this approach the Government seeks to ensure that it can obtain the benefits of new design enhancements and technological updates or advances to hardware products currently under contract. When requested or offered, the Contractor shall provide, within thirty (30) calendar days of receipt of request, an ECP for the applicable new or enhanced hardware technology for Technology Refresh or Technology Insertion. The Government reserves the ultimate authority to approve, or disapprove, ECPs whether they are submitted to support Technology Refresh or Technology Insertion. This approval is at the sole discretion of the CO.

In the event that the Contractor is no longer able to provide IT hardware commodity products under the Contract due to end of life, obsolescence or other reason, the Contractor may, with notification to and approval by the Government, remove the products from the contract. Upon Government approval the Contractor shall submit an ECP for Technology Refresh identifying substitute products which shall meet the applicable hardware technical functional area specification requirements. However, the product prices proposed, and incorporated into the CEC Contract are binding and thereby establish the Government's maximum liability for said product over the life of the Contract. Therefore, the price of the product(s) refreshed, including support services, shall not exceed the price proposed, and incorporated into the basic Contract, for the product being refreshed.

An ECP is a proposed engineering change and the documentation by which the change is described, justified, and submitted to the VA for approval or disapproval.

There are two (2) classifications of ECP's as defined below:

Major ECP

Major ECPs apply to:

- Products introduced by the VA or Contractor that result from the requirement for Technology Insertion.
- Products provided by the Contractor that have undergone major component, configuration, and/or system changes.
- Any introduced product or product change that may impact the ability to meet performance specifications, the connectivity and/or interoperability with current VA systems.
- Any product change that will result in a favorable reduction in price, or improved performance.

The CO may ask the Contractor to prepare a Major ECP for new technical functional area hardware items within the scope of this Contract. Upon receipt of a written request from the CO, the Contractor shall prepare and submit an ECP in accordance with the information provided below.

The Contractor may also initiate a Major ECP. Any Major ECP submitted to the CO shall include technical, price, and delivery terms that need to be negotiated prior to issuing a modification for incorporation of the change.

After submission of a Contractor-initiated Major ECP, the CO may require the Contractor to submit the following information:

- Cost or pricing data in accordance with FAR 15.403-5 if the proposed change meets the criteria for its submission under FAR 15.403-4 or current commercial or other published price list.
- Information other than cost or pricing data adequate for the CO to make a determination of price reasonableness. The CO reserves the right to request additional information if that provided by the Contractor is considered inadequate for that purpose. If the Contractor claims applicability of one of the exceptions to submission of cost or pricing data, it shall cite the exception and provide rationale for its applicability.

A Major ECP submitted to the VA for approval shall contain, at a minimum, the following information:

1. Title
2. Company Name, Name of individual submitting ECP, title and contact information.
3. Technical Functional Area Hardware Identification and applicable Contract Line Item Number (CLIN)
4. Description of Problem/Deficiency
5. Justification for Change
6. Description of Proposed Solution / Alternative (to include compliance with the specification for the affected technical functional area).
7. Supporting Information (to include evidence that proposed price equates to or is better than the price discount for the hardware product currently under contract).
8. Prepared By
9. POC Information

Minor ECP

Minor ECP's apply to:

- Any minor component, configuration, and/or system change that does not impact the ability to meet performance specifications, connectivity and/or interoperability with current VA systems.
- Model Number Changes.

The Contractor may initiate a Minor ECP. All Minor ECPs shall be submitted to the CO as a notice that a minor change has taken effect.

A Minor ECP provided to the VA shall contain, at a minimum, the following information:

1. Title
2. Company Name, Name of individual submitting ECP, title and contact information.
3. Technical Functional Area Hardware Identification
4. Description of Problem/Deficiency

5. Justification for Change
6. Description of Proposed Solution / Alternative
7. Supporting Information
8. Prepared By
9. POC Information

Upon review of any Major or Minor ECP submission, the Government shall have the right to approve any or all of the proposed changes for incorporation into the contract, including new or substitution CLINs and to unilaterally modify the contract to provide for order of new or replacement technology hardware. Likewise, the Government reserves the right to reject any proposed ECP, at no cost to the Government.

Windows OS Laptop - Tablet			
Laptop(Tablet) - Technical Specification		Minimum Requirements	
General Requirement - Model Proposed (Please include manufacturer's part number)		OEM & Model/Part Number:	
Reference Number	Parameter	Attribute	Value
1	Processor	Minimum Speed (Ghz)	2.5 Ghz
2		TPM Support: Desktop and Mobile Architecture for System Hardware (DASH) 1.1 or equivalent to include either Intel's vPro or AMD's DASH 1.1 compliant	YES
3	Memory	Minimum Speed (Mhz)	1333 Mhz
4		Minimum (GB)	4
5	Display / Graphics	Screen Size, Minimum (inches)	12.1
6		Minimum Resolution (pixels, h x v)	1280X768
7		Acceptable aspect ratios	16:9 or 16:10
8		Integrated graphics acceptable	YES
9		Dedicated video memory required	NO
10		Shared video memory accepted	YES
11		Graphics memory, mimimum	512 MB
12	Mouse	Multi-touch touchpad/pointer stick	Required
13	Speaker	Internal	YES
14	Networking	Wireless	802.11g/n
15		NIC speed, minimum (gbps)	1 GB
16		Support for FIPS 140-2 and IEEE 802.11	YES
17	USB 2.0	number of ports, minimum	3
18	Primary Hard Drive	Interface	SATA
19		Capacity, minimum (GB)	250 GB
20		RPM, minimum	4200
21	Optical Device	Interface for external CD/DVD	YES
22	Battery/AC Adapter	Cells, minimum	6 cell count and required to support a minimum run time, on battery, of 5 hours
23		EPA Energy Star rated	YES
24	Security	Smart card reader (Internal)	YES
25	Operating Systems Supported	Windows 7, Enterprise Ed.	YES
26		MS Certified for Win 7 (32 and 64 bit)	YES
27	Docking Station	Interface for port replicator	YES

Windows OS Laptop - Light

Windows OS Laptop - Light			
Laptop(Light) - Technical Specification		Minimum Requirements	
General Requirement - Model Proposed (Please include manufacturer's part number)		OEM & Model/Part Number:	
Reference Number	Parameter	Attribute	Value
1	Processor	<i>Minimum Speed (Ghz)</i>	2.5Ghz
2		<i>TPM Support: Desktop and Mobile Architecture for System Hardware (DASH) 1.1 or equivalent to include either Intel's vPro or AMD's DASH 1.1 compliant</i>	YES
3		<i>Minimum Number of Cores</i>	2
4	Memory	<i>Minimum Speed (Mhz)</i>	1333 Minimum
5		<i>Minimum (GB)</i>	4
6	Display / Graphics	<i>Screen Size, Minimum (inches)</i>	12.1
7		<i>Minimum Resolution (pixels, h x v)</i>	1366X768 (or greater)
8		<i>Acceptable aspect ratios</i>	16:9 or 16:10
9		<i>Integrated graphics acceptable</i>	YES
10		<i>Dedicated video memory required</i>	NO
11		<i>Shared video memory accepted</i>	YES
12		<i>Graphics memory, minimum</i>	512 MB
13	Mouse	<i>Multi-touch touchpad/pointer stick</i>	Required
14	Speaker	<i>Internal</i>	YES
15	Networking	<i>Wireless</i>	802.11g/n
16		<i>NIC speed, minimum (gbps)</i>	1 GB
17		<i>Support for FIPS 140-2 and IEEE 802.11</i>	YES
18	USB 2.0	<i>number of ports, minimum</i>	2
19	Primary Hard Drive	<i>Interface</i>	SATA
20		<i>Capacity, minimum</i>	250 GB
21		<i>RPM, minimum</i>	7200
22	Integrated Camera, 720p HD resolution	<i>Present</i>	YES
23	Optical Device	<i>Interface for external CD/DVD</i>	YES
24	Battery/AC Adapter	<i>Cells, minimum</i>	cell count required to support a minimum run time, on battery, of 5 hours
25		<i>EPA Energy Star rated</i>	YES
26	Security	<i>Smart card reader (Internal)</i>	YES
27	Operating Systems Supported	<i>Windows 7, Enterprise Ed.</i>	YES
28		<i>MS Certified for Win 7 (32 and 64 bit)</i>	YES
29	Docking Station	<i>Interface for port replicator</i>	YES

Windows OS Laptop - Medium			
Laptop(Medium) - Technical Specification		Minimum Requirements	
General Requirement - Model Proposed (Please include manufacturer's part number)		OEM & Model/Part Number:	
Reference Number	Parameter	Attribute	Value
1	Processor	Minimum Speed (Ghz)	2.5 Ghz
2		TPM Support: Desktop and Mobile Architecture for System Hardware (DASH) 1.1 or equivalent to include either Intel's vPro or AMD's DASH 1.1 compliant	YES
3		Minimum Number of Cores	2
4	Memory	Minimum Speed (Mhz)	1333 Minimum
5		Minimum (GB)	4
6	Display / Graphics	Screen Size, Minimum (inches)	14
7		Minimum Resolution (pixels, h x v)	1366X768
8		Acceptable aspect ratios	16:9 or 16:10
9		Integrated graphics acceptable	YES
10		Dedicated video memory required	NO
11		Shared video memory accepted	YES
12		Graphics memory, minimum	512 MB
13		Dual-head/link support	YES
14	Networking	Wireless	802.11g/n
15		NIC speed, minimum (gbps)	1 GB
16		Support for FIPS 140-2 and IEEE 802.11	YES
17	Monitor	Privacy Filter	YES
18	Speaker	Internal	YES
19	Keyboard	Smart keyboard	YES
20		USB connected	YES
21	Integrated Features	Hot buttons/hot key sequence to permit enabling/disabling of wireless networks, speaker, external monitor	YES
22		Hot button/hot key sequence to permit enabling/disabling of touchpad	YES
23	Mouse	Multi-touch touchpad/pointer stick	Required
24	Keyboard Illumination	Backlit or other <u>integrated</u> keyboard lighting system	YES
25	USB 2.0	number of ports, minimum	3
26	Integrated Camera, 720p HD resolution	Present	YES
27	Primary Hard Drive	Interface	SATA
28		Capacity, minimum (GB)	250
29		RPM, minimum	7200
30	Optical Device	8X DVD +/- RW	YES
31	Battery/AC Adapter	Cells, minimum	cell count required to support a minimum run time, on battery, of 5 hours
32		EPA Energy Star rated	YES
33	Security	Smart card reader (Internal)	YES
34	Operating Systems Supported	Windows 7, Enterprise Ed.	YES
35		MS Certified for Win 7 (32 and 64 bit)	YES
36	Docking Station	Interface for port replicator	YES
37		* VA requires 2 video outputs, either one of each or one VGA and multiple on the Digital on the larger docks is acceptable.	YES

Windows OS Laptop - Heavy			
Laptop(Heavy) - Technical Specification		Minimum Requirements	
General Requirement - Model Proposed (Please include manufacturer's part number)		OEM & Model/Part Number:	
Reference Number	Parameter	Attribute	Value
1	Processor	<i>Minimum Speed (Ghz)</i>	2.5
2		<i>TPM Support: Desktop and Mobile Architecture for System Hardware (DASH) 1.1 or equivalent to include either Intel's vPro or AMD's DASH 1.1 compliant</i>	YES
3		<i>Number of Cores</i>	QUAD
4	Memory	<i>Minimum Speed (Mhz)</i>	1333
5		<i>Minimum (GB)</i>	4
6	Display / Graphics	<i>Screen Size, Minimum (inches)</i>	17
7		<i>Minimum Resolution (pixels, h x v)</i>	1920x1080
8		<i>Acceptable aspect ratios</i>	16:9 or 16:10
9		<i>Graphics memory, minimum</i>	512 MB
10		<i>Dedicated video memory required</i>	YES
11		<i>Shared video memory accepted</i>	NO
12		<i>Dual-head support</i>	YES
13	Speaker	<i>Internal</i>	YES
14	Integrated Features	<i>Hot buttons/hot key sequence to permit enabling/disabling of wireless networks, speaker, external monitor</i>	YES
15		<i>Hot button/hot key sequence to permit enabling/disabling of touchpad</i>	YES
16	Mouse	<i>Multi-touch touchpad/pointer stick</i>	Required
17	Networking	<i>Wireless</i>	802.11g/n
18		<i>NIC speed, minimum (gbps)</i>	1
19		<i>Support for FIPS 140-2 and IEEE 802.11</i>	YES
20	USB 2.0	<i>number of ports, minimum</i>	4
21	Integrated Camera, 720p HD resolution	<i>present</i>	YES
22	Primary Hard Drive	<i>Interface</i>	SATA
23		<i>Capacity, minimum (GB)</i>	250
24		<i>RPM, minimum</i>	7200
25	Optical Device	<i>8X DVD +/- RW</i>	YES
26	Battery/AC Adapter	<i>Cells, minimum</i>	cell count required to support a minimum run time, on battery, of 5 hours
27		<i>EPA Energy Star rated</i>	YES
28	Security	<i>Smart card reader (Internal)</i>	YES
29	Operating Systems Supported	<i>Windows 7, Enterprise Ed.</i>	YES
30		<i>MS Certified for Win 7 (32 and 64 bit)</i>	YES
31	Docking Station	<i>Interface for port replicator</i>	YES

Windows OS Laptop - Semi-Rugged			
Laptop (Semi-Rugged) - Technical Specification		Minimum Requirements	
General Requirement - Model Proposed (Please include manufacturer's part number)		OEM & Model/Part Number:	
Reference Number	Parameter	Attribute	Value
1	Processor	Minimum Speed (Ghz)	2.5 Ghz
2		TPM Support: Desktop and Mobile Architecture for System Hardware (DASH) 1.1 or equivalent to include either Intel's vPro or AMD's DASH 1.1 compliant	YES
3	Memory	Minimum Number of Cores	2
4		Minimum Speed (Mhz)	1066
5		Minimum (GB)	4
6		Screen Size, Minimum (inches)	14
7	Display / Graphics	Minimum Resolution (pixels, h x v)	1366X768
8		Acceptable aspect ratios	16:9 or 16:10
9		Integrated graphics card	YES
10		Graphics memory, minimum	512 MB
11	Networking	Dedicated video memory required	NO
12		Shared video memory accepted	YES
13		Wireless	802.11g/n
14		NIC speed, minimum (gbps)	1 GB
15	Keyboard and Input	Support for FIPS 140-2 and IEEE 802.11	YES
16		LED Backlighting	YES
17		Touchscreen LCD	YES
18		Keyboard Standard Sealed (to prevent water/dust damage)	YES
19	Mouse	protective keyboard membrane	YES
20		Multi-touch touchpad	Required
21	USB 2.0	number of ports, minimum	4
22	Speaker	Internal	YES
23	Integrated Camera, 720p HD resolution	Present	YES
24	Primary Hard Drive	Interface	SATA
25		Capacity, minimum (GB)	250
26		RPM, minimum	5400
27	Optical Device	Internal CD/DVD	YES
28	Battery/AC Adapter		cell count required to support a minimum run time, on battery, of 5 hours
29		Cells, minimum	
30	Security	EPA Energy Star rated	YES
31		Smart card reader (Internal)	YES
32	Operating Systems Supported	Kensington Cable Lock slot	YES
33		Windows 7, Enterprise Ed.	YES
34	Durability Features	MS Certified for Win 7 (32 and 64 bit)	YES
		* Modified drop resistant (from heights of 29 inches)	YES
		* High-altitude pressure resistant	
		* Vibration resistant	
		* Splash resistant	
		* Dust resistant	
		* Operational temperature of -5 deg to 120 deg Farenheit	YES
35	Integrated Options	Port covers	YES
36		Backlit or front-lit keyboard lighting system	YES
37		Interface for Port Replicator	YES

Mac OS Laptop - Medium			
		Model/Part Number of machines that meet minimum requirements:	
Technical Specification			Minimum Requirements
General Requirement			
Reference Number	Parameter	Attribute	Medium (2.2GHz)
1	Processor	<i>Minimum Speed (Ghz)</i>	2.2
2		<i>Number of Cores</i>	DUAL
3	Memory	<i>Minimum Speed (MHz)</i>	800
4		<i>Minimum (GB)</i>	4
5	Display / Graphics	<i>Screen Size, Minimum (inches)</i>	14"
6		<i>Minimum Resolution (pixels, h x v)</i>	1440X900
7		<i>Integrated graphics card</i>	YES
8		<i>Integrated graphics card Memory, minimum</i>	384
9		<i>Discrete graphics card</i>	YES
10		<i>Discrete graphics card Memore, minimum</i>	1 GB
11		<i>Wireless</i>	A+B+G+N
12	Mouse	<i>Multi-touch touchpad/pointer stick</i>	Required
13	Networking	<i>NIC speed, minimum (gbps)</i>	1
14		<i>Support for FIPS 140-2 and IEEE 802.11</i>	YES
15	BACKLIT KEYBOARD	<i>Backlit</i>	YES
16	WIRED KEYBOARD	<i>Integrated or wired - no wireless</i>	YES - integrated
17	USB 2.0	<i>number of ports, minimum</i>	2
18	Integrated Camera, 720p	<i>Present</i>	YES
19	Primary Hard Drive	<i>Interface</i>	SATA
20		<i>Capacity, minimum (GB)</i>	320
21		<i>RPM, minimum</i>	5400
22	Optical Device	<i>8X DVD +/- RW</i>	YES
23	Battery/AC Adapter	<i>Cells, minimum</i>	Cell count required to support a minimum run time, on battery, of 5 hours
24		<i>EPA Energy Star rated</i>	YES
25	Operating Systems Supported	<i>OS X (latest commercially supported, e.g. 10.6 Snow Leopard or 10.7 Lion)</i>	YES
26		<i>REQUIREMENT DELETED</i>	

Mac OS Laptop - Heavy			
		Model/Part Number of machines that meet minimum requirements:	
Technical Specification			Minimum Requirements
General Requirement			Laptop Heavy
Reference Number	Parameter	Attribute	
1	Processor	Minimum Speed (Ghz)	2.2
2		Number of Cores	QUAD
3	Memory	Minimum Speed (MHz)	800
4		Minimum (GB)	4
5	Display / Graphics	Screen Size, Minimum (inches)	17
6		Minimum Resolution (pixels, h x v)	1920x1200
7		Integrated graphics card	YES
8		Integrated graphics card Memory, minimum	384
9		Discrete graphics card	YES
10		Discrete graphics card Memore, minimum	1
11		Wireless	A+B+G+N
12	Mouse	Multi-touch touchpad/pointer stick	Required
13	Networking	NIC speed, minimum (gbps)	1
14		Support for FIPS 140-2 and IEEE 802.11	YES
15	BACKLIT KEYBOARD	Backlit	YES
16	WIRED KEYBOARD	Integrated or wired - no wireless	YES - integrated
17	USB 2.0	number of ports, minimum	2
18	Integrated Camera, 720p	Present	YES
19	Primary Hard Drive	Interface	SATA
20		Capacity, minimum (GB)	500
21		RPM, minimum	5400
22	Optical Device	8X DVD +/- RW	YES
23	Battery/AC Adapter	Cells, minimum	Cell count required to support a minimum run time, on battery, of 5 hours
24		EPA Energy Star rated	YES
25	Operating Systems Supported	OS X (latest commercially supported, e.g. 10.6 Snow Leopard or 10.7 Lion)	YES
26		REQUIREMENT DELETED	

Mac OS Desktop			
		Model/Part Number of machines that meet minimum requirements:	
Technical Specification			Minimum Requirements
General Requirement			Desktop
Reference Number	Parameter	Attribute	All- in- One
1	Processor	<i>Minimum Speed (Ghz)</i>	2.5
2		<i>Number of Cores</i>	QUAD
3	Memory	<i>Minimum Speed (Mhz)</i>	1333
4		<i>Minimum (GB)</i>	4
5	Display / Graphics	<i>Screen Size, Minimum (inches)</i>	21
6		<i>Minimum Resolution (pixels, h x v)</i>	1920x1080
7		REQUIREMENT DELETED	
8		REQUIREMENT DELETED	
9		<i>Discrete graphics card</i>	YES
10		<i>Discrete graphics card Memore, minimum</i>	512
11		<i>Wireless</i>	A+B+G+N
12	Mouse	<i>Multi-touch touchpad/pointer stick</i>	Required
13	Networking	<i>NIC speed, minimum (gbps)</i>	1
14		<i>Support for FIPS 140-2 and IEEE 802.11</i>	YES
15	BACKLIT KEYBOARD	<i>Backlit</i>	NO
16	WIRED KEYBOARD	<i>Integrated or wired - no wireless</i>	YES - must be specified.
17	USB 2.0	<i>number of ports, minimum</i>	4
18	Integrated Camera, 2.0MP	<i>Present</i>	YES
19	Primary Hard Drive	<i>Interface</i>	SATA
20		<i>Capacity, minimum (GB)</i>	500
21		<i>RPM, minimum</i>	7200
22	Optical Device	<i>8X DVD +/- RW</i>	YES
23	Battery/AC Adapter	<i>Cells, minimum</i>	NA
24		<i>EPA Energy Star rated</i>	YES
25	Operating Systems Supported	<i>OS X (latest commercially supported, e.g. 10.6 Snow Leopard or 10.7 Lion)</i>	YES
26		REQUIREMENT DELETED	

Windows OS Thin Client			
Thin Client - Technical Specification		Minimum Requirements	
General Requirement - Model Proposed (Please include manufacturer's part number)		OEM and Model/Part Number:	
Reference Number	Parameter	Attribute	Value
1	Processor	Minimum Speed (Ghz)	1Ghz
2	Memory	DDR (Minimum)	2GB
3		Flash (Minimum)	2GB
4	Display / Graphics	Display (Dual Display Support)	1 VGA/1 DVI
5		Resolution Support minimum	1680x1050
6	Mouse	USB	Y
7	Keyboard	USB	Y
8	Networking	Wireless (Optional)	802.11 g/n
9		Ethernet - 10/100/1000 Gigabit	Y
10		Support for FIPS 140-2 and IEEE 802.11	Y
11	Media Drive	CD/DVD	N
12	USB 2.0	Number of ports, minimum	6
13	Power In	EPA Energy Star rated	Y
14	Security	Smart card reader (Internal/external)	Y
15		(if external card reader it cannot take one of the required USD ports)	
16	Height	Minimum	7"
17	Width	Minimum	1"
18	Depth	Minimum	8"
19	Operating Systems Supported	Windows Embedded Standard 7	
20	Virtualization Platforms Supported	Citrix/Vmware/Microsoft	

Monitors - Small			
Technical Specification		Minimum Requirements	
General Requirement - Model Proposed (Please include manufacturer's part number)		Model/Part Number:	
Reference Number	Parameter	Attribute	Value
1	Display	Minimum Viewable Size	18.5"
2	Display	Type	Widescreen
3	Display	Resolution (Minimum)	1366x768
4	Display	Display Position Adjustments	Tilt
5	Display	Minimum Response Time	5ms
6	Display	Aspect Ratio	16x9
7	Interface	VGA Input	Yes
8	Interface	DVI-D Input	Yes
9	Environmental	Energy Star Qualified	Yes

Monitors - Large			
Technical Specification		Minimum Requirements	
General Requirement - Model Proposed (Please include manufacturer's part number)		Model/Part Number:	
Reference Number	Parameter	Attribute	Value
1	Display	Minimum Viewable Size	21.5"
2	Display	Type	Widescreen
3	Display	Resolution (Minimum)	1920x1080
4	Display	Display Position Adjustments	Tilt
5	Display	Minimum Response Time	5ms
6	Display	Aspect Ratio	16x9
7	Interface	VGA Input	Yes
8	Interface	DVI-D Input	Yes
9	Environmental	Energy Star Qualified	Yes

Docking Station - Windows OS Laptop Tablet			
Technical Specification		Minimum Requirements	
General Requirement - Model Proposed (Please include manufacturer's part number)		Model/Part Number:	
Reference Number	Parameter	Attribute	Value
1	Docking Station	Interface for port replicator	YES
2		REQUIREMENT DELETED	
3		Support for dual external monitors	YES
4		two (2) display ports, such as HDMI, VGA, DVI, and/or DisplayPort	YES
5		USB ports	4
6		Port for locking device to secure laptop to dock/replicator required	YES
7		Port for locking device to secure docking station/replicator to a fixed object (desk)	YES
8		NIC port	YES
9		Printer/Com Port	YES
10		Integrated 10/100 Ethernet LAN with RJ45 connector	YES
11		REQUIREMENT DELETED	

Docking Station - Windows OS Laptop Light			
Technical Specification		Minimum Requirements	
General Requirement - Model Proposed (Please include manufacturer's part number)		Model/Part Number:	
Reference Number	Parameter	Attribute	Value
1	Docking Station	Interface for port replicator	YES
2		REQUIREMENT DELETED	
3		Support for dual external monitors	YES
4		two (2) display ports, such as HDMI, VGA, DVI, and/or DisplayPort	YES
5		USB ports	5
6		Port for locking device to secure laptop to dock/replicator required	YES
7		Port for locking device to secure docking station/replicator to a fixed object (desk)	YES
8		NIC port	YES
9		Printer/Com Port	YES
10		Integrated 10/100 Ethernet LAN with RJ45 connector	YES
11		REQUIREMENT DELETED	

Docking Station - Windows OS Laptop Medium			
Technical Specification		Minimum Requirements	
General Requirement - Model Proposed (Please include manufacturer's part number)		Model/Part Number:	
Reference Number	Parameter	Attribute	Value
1	Docking Station	Interface for port replicator	YES
2		REQUIREMENT DELETED	
3		Support for dual external monitors	YES
4		two (2) display ports, such as HDMI, VGA, DVI, and/or DisplayPort	YES
5		USB ports	5
6		Port for locking device to secure laptop to dock/replicator required	YES
7		Port for locking device to secure docking station/replicator to a fixed object (desk)	YES
8		NIC port	YES
9		Printer/Com Port	YES
10		Integrated 10/100 Ethernet LAN with RJ45 connector	YES
11		REQUIREMENT DELETED	

Docking Station - Windows OS Laptop Heavy			
Technical Specification		Minimum Requirements	
General Requirement - Model Proposed (Please include manufacturer's part number)		Model/Part Number:	
Reference Number	Parameter	Attribute	Value
1	Docking Station	Interface for port replicator	YES
2		REQUIREMENT DELETED	
3		Support for dual external monitors	YES
4		two (2) display ports, such as HDMI, VGA, DVI, and/or DisplayPort	YES
5		USB ports	5
6		Port for locking device to secure laptop to dock/replicator required	YES
7		Port for locking device to secure docking station/replicator to a fixed object (desk)	YES
8		NIC port	YES
9		Printer/Com Port	YES
10		Integrated 10/100 Ethernet LAN with RJ45 connector	YES
11		REQUIREMENT DELETED	

Docking Station - Windows OS Laptop Semi-Rugged			
Technical Specification			
General Requirement - Model Proposed (Please include manufacturer's part number)		Minimum Requirements	
Reference Number	Parameter	Attribute	Value
1	Docking Station	Interface for port replicator	YES
2		REQUIREMENT DELETED	
3		Support for dual external monitors	YES
4		two (2) display ports, such as HDMI, VGA, DVI, and/or DisplayPort	YES
5		USB ports	5
6		Port for locking device to secure laptop to dock/replicator required	YES
7		Port for locking device to secure docking station/replicator to a fixed object (desk)	YES
8		NIC port	YES
9		Printer/Com Port	YES
10		Integrated 10/100 Ethernet LAN with RJ45 connector	YES
		REQUIREMENT DELETED	

Docking Station - Mac OS Laptop Medium			
Technical Specification		Minimum Requirements	
General Requirement - Model Proposed (Please include manufacturer's part number)		Model/Part Number:	
Reference Number	Parameter	Attribute	Value
1	Docking Station	Interface for port replicator	YES
2		REQUIREMENT DELETED	
3		REQUIREMENT DELETED	
4		One (1) display port, such as HDMI, VGA, DVI, and/or DisplayPort	YES
5		USB ports	5
6		Access to port for locking device to secure laptop to the desk when laptop is docked in dock/replicator	YES
7		REQUIREMENT DELETED	YES
8		NIC port	YES
9		Printer/Com Port (may use USB port)	YES
10		Integrated 10/100 Ethernet LAN with RJ45 connector	YES
11		REQUIREMENT DELETED	

Docking Station - Mac OS Laptop Heavy			
Technical Specification		Minimum Requirements	
General Requirement - Model Proposed (Please include manufacturer's part number)		Model/Part Number:	
Reference Number	Parameter	Attribute	Value
1	Docking Station	Interface for port replicator	YES
2		REQUIREMENT DELETED	
3		REQUIREMENT DELETED	
4		One (1) display port, such as HDMI, VGA, DVI, and/or DisplayPort	YES
5		USB ports	5
6		Access to port for locking device to secure laptop to the desk when laptop is docked in dock/replicator	YES
7		REQUIREMENT DELETED	YES
8		NIC port	YES
9		Printer/Com Port (may use USB port)	YES
10		Integrated 10/100 Ethernet LAN with RJ45 connector	YES
11		REQUIREMENT DELETED	

Android Type 1 Option 1			
Tablet - Technical Specification		OEM & Model/Part Number, Option 1:	
General Requirement - Model Proposed		Minimum Requirements	Option 1
Reference Number	Parameter	Attribute	Value
1	Processor	Minimum Speed (Ghz)	1
2		Number of Cores	DUAL
3	Display / Graphics	Screen Size (inches)	7
4		Minimum Resolution (pixels, h x v)	1280x800
5	Networking	Wireless	A+B+G+N
6		Cellular	3G* or 4G*
7	Bluetooth	Present	YES
8		NO REQUIREMENT	
9	Integrated Camera	Present	YES
10		Back Camera (video recording) minimum	720P (3MP)
11		Front Camera (video recording) minimum	VGA (2MP)
12	Integrated Microphone	Present	YES
13	Storage	Capacity, minimum (GB)	16
14		Removable	YES
15		Encrypted	NO
16	Operating Systems Supported	Android 3.1 (Honeycomb)	YES
17		Support native Android Market	YES
18	Security	Full Device Encryption (FIPS Standards)	NO
19		Support for Strong Passwords to access device	YES
20	Email	Support for Secure Exchange Active Sync	YES
21	Dock Connector	Supports HDMI, USB, and power	YES
22	Power	Batteries and Charger included	YES

* Either LTE, HSPA or WiMax

Android Type 1 Option 2			
Tablet - Technical Specification		OEM & Model/Part Number, Option 2:	
General Requirement - Model Proposed		Minimum Requirements	Option 2
Reference Number	Parameter	Attribute	Value
1	Processor	Minimum Speed (Ghz)	1
2		Number of Cores	DUAL
3	Display / Graphics	Screen Size (inches)	9 (minimum)
4		Minimum Resolution (pixels, h x v)	1280x800
5	Networking	Wireless	A+B+G+N
6		Cellular	3G* or 4G*
7	Bluetooth	Present	YES
8		NO REQUIREMENT	
9	Integrated Camera	Present	YES
10		Back Camera (video recording) minimum	720P (3MP)
11		Front Camera (video recording) minimum	VGA (2MP)
12	Integrated Microphone	Present	YES
13	Storage	Capacity, minimum (GB)	16
14		Removable	YES
15		Encrypted	NO
16	Operating Systems Supported	Android 3.1 (Honeycomb)	YES
17		Support native Android Market	YES
18	Security	Full Device Encryption (FIPS Standards)	NO
19		Support for Strong Passwords to access device	YES
20	Email	Support for Secure Exchange Active Sync	YES
21	Dock Connector	Supports HDMI, USB, and power	YES
22	Power	Batteries and Charger included	YES

* Either LTE, HSPA or WiMax

iPad Type 2A Wi-Fi			
OEM & Model/Part Number:			
Tablet - Technical Specification		Minimum Requirements	Type 2A, Wi-Fi
Reference Number	Parameter	Attribute	Value
1	Processor	1GHz dual-core Apple A5	1
2		Number of Cores	2
3	Display / Graphics	Screen Size, Minimum (inches)	9
4		Minimum Resolution (pixels, h x v)	1024X768
5	Networking	802.11	A+B+G+N
6		Cellular	NO
7	Bluetooth	Present	YES
8		NO REQUIREMENT	
9	Integrated Camera	Present	YES
10		Back Camera (video recording) minimum	HD (720P)
11		Front Camera (video recording) minimum	VGA (30 frames per second)
12	Integrated Microphone	Present	YES
13	Storage	Capacity, minimum (GB)	16
14		Removable	NO
15		Encrypted	NO
16	Operating Systems Supported	iOS5.0	5.0
17		REQUIREMENT DELETED	
18	Security	Full Device Encryption (FIPS Standards)	NO
19		Support for Strong Passwords to access device	YES
20	Email	Support for Secure Exchange Active Sync	YES
21	Dock Connector	Supports HDMI, USB, and power	YES
22	Power	Batteries and Charger included	YES

iPad Type 2B 3G			
OEM & Model/Part Number:			
Tablet - Technical Specification		Minimum Requirements	Type 2B, 3G
Reference Number	Parameter	Attribute	
1	Processor	1GHz dual-core Apple A5	1
2		Number of Cores	2
3	Display / Graphics	Screen Size, Minimum (inches)	9
4		Minimum Resolution (pixels, h x v)	1024X768
5	Networking	802.11	A+B+G+N
6		Cellular	3G
7	Bluetooth	Present	YES
8		NO REQUIREMENT	
9	Integrated Camera	Present	YES
10		Back Camera (video recording) minimum	HD (720P)
11		Front Camera (video recording) minimum	VGA (30 frames per second)
12	Integrated Microphone	Present	YES
13	Storage	Capacity, minimum (GB)	16
14		Removable	NO
15		Encrypted	NO
16	Operating Systems Supported	iOS5.0	5.0
17		REQUIREMENT DELETED	
18	Security	Full Device Encryption (FIPS Standards)	NO
19		Support for Strong Passwords to access device	YES
20	Email	Support for Secure Exchange Active Sync	YES
21	Dock Connector	Supports HDMI, USB, and power	YES
22	Power	Batteries and Charger included	YES

Blackberry - Type 3 - Option 1			
Tablet - Technical Specification		OEM & Model/Part Number:	
General Requirement - Model Proposed (Please include manufacturer's part number)		Minimum Requirements	Option 1, Wi-Fi
Reference Number	Parameter	Attribute	Value
1	Processor	Minimum Speed (Ghz)	1
2		Number of Cores	DUAL
3	Display / Graphics	Screen Size, Minimum (inches)	7
4		Minimum Resolution (pixels, h x v)	1024x600
5	Networking	Wireless	A+B+G+N
6		Cellular	NO
7	Bluetooth	Present	YES
8		NO REQUIREMENT	
9	Integrated Camera	Present	YES
10		Back Camera (video recording) minimum	5MP
11		Front Camera (video recording) minimum	3MP
12	Integrated Microphone	Present	YES
13	Storage	Capacity, minimum (GB)	16
14		Removable	NO
15		Encrypted	YES
16	Operating Systems Supported	BlackBerry Tablet OS	YES
17		NO REQUIREMENT	
18	Security	Full Device Encryption (FIPS Standards)	YES
19		Support for Strong Passwords to access device	YES
20	Email	Support for Secure Exchange Active Sync	YES
21	Dock Connector	Supports HDMI, USB, and power	YES
22	Power	Batteries and Charger included	YES

	Heavy Workload Server (Class A) - Rack	
	OEM & Model/Part Number:	
Reference Number	Requirement	Rack Mount Server
1	Solution must provide x86 or x64 processor. The solution requires the minimum number of processor sockets on the server.	>=2
2	Solution must meet performance capacity with the minimum value within the SPEC INT_RATE_BASE 2006 benchmark test. This should be demonstrated via published benchmark results applicable to the specific server configuration.	>=300
3	Solution must support a minimum Socket Count of which meets the Performance Benchmark Standards (found in reference 2)	Y
4	Solution must support a core count at a minimal amount to meet the Performance Benchmark Standards. (found in reference 2)	Y
5	Solution requires the minimum cores per processor as specified in the SPEC Benchmark Standard. (found in reference 2)	Y
6	Solution must have minimal Socket Count due to licensing cost per socket, and have minimum count for performance/capacity	Y
7	Solution must have minimum Core count expected for performance / capacity, level is equal to quad-core. Any amount that meets the Performance Benchmark Standards is sufficient	Y
8	Solution requires at minimum, the following GB of RAM. RAM must be compatible with CPU and full error correction functionality to include ECC. All memory modules must be the same type and size. All memory must be installed in a manner to take full advantage of processor capabilities.	128GB
9	Solution requires that all memory channels must be symmetrically populated to achieve memory bandwidth of referenced performance benchmark	Y
10	Solution requires at minimum 25% of the provided DIMM slots to be unpopulated at time of delivery.	Y
11	The solution must support at minimum, the following sustainable throughput IOs per second.	375 IOPs
12	Rack Mounted Server should not exceed (4U) in size and fit in an "industry standard" 42U rack without special modifications to the rack and/or server. The server mount brackets should be "generic" for all types of 42U racks. Rail type: Tool-less square-hole sliding. Cable: Side-reversible for non-blade solutions.	Y
13	Rack mount type	4U max

14	The solution must be a rack or blade (specified at time of delivery order) server. If Rack mounted server, the rail type will be tool-less square-holes (default is RACK)	Y
15	(1) Hard drive raid controller that will support at minimum RAID1 and "hot spare" automatic drive rebuild functionality for (at minimum) RAID1 for "Rack Mount Servers". When server is configured as a transaction server, a separate RAID Controller or second channel on the same controller is required for the "temp file" RAID group. Must support SAS drives.	Y
16	The solution must support RAID 1 for Blade Servers. Must support SAS drives.	N
17	The solution is required to have a minimum Controller Cache of 256MB. Blade Servers are only mandatory if not being virtualized. If virtualized, they will be boot from SAN.	Y
18	The solution must support a minimum of 1 Controller.	Y
19	The solution must support a minimum private 32KB L1 instructional cache and private 32KB L1 data cache for each processor core. Minimum 256KB L2 cache per core. 6MB or greater shared L3 cache.	Y
20	The solution must support processors capable of Symmetrical multi processing.	Y
21	Solution must support at minimum the following number of network interface cards with TCP checksum offload functionality. for Windows only.	4
22	Solution must support a minimum network port count of 2. More may be required dependant on virtual infrastructure requirements (to be specified at time of delivery order), for Rack Mount Servers Only.	Y
23	Solution must support a minimum of 1GB of Bandwidth.	Y
24	Solution must support dual imbedded switches for Blade Chassis components for Blade Servers.	N
25	For Virtual Environments only, solution must support a base set of 4 ports to be used for virtual guests, 1 for the console, 1 for the live migration. Additional may be required dependant on the profile of workload/application. For Rack Mount Servers Only.	Y
26	Solution must support a base set of 2 ports or more for cluster interconnects dependant on cluster traffic. For Cluster Environments. Number required...(minimum is 2)	Y
27	Solution must support embedded port count of one "card", all interfaces used are spread across two "cards" (to include at least on add-on NIC). The goal is physical separation of the chipset / ASIC used on the redundant port, for each function. Support for "simple failover" (with a single IP address) and independent usage (with multiple IP addresses) is required.	Y

28	Solution must provide a minimum of (3) internal hard drives with average throughput of 80 MB/s with no greater than 4ms latency. Drives must support 3ms read times and 4ms write times. In support of this solution, the drives must provide at minimum the application specific (provided at time of delivery order) usable disk space.	Y
29	Solution for Blade Servers will consist of Number required...(the required amount is 2) Internal Hard Drives with an average throughput of 80MB/s with no greater than 4ms latency. Drives must support 3ms read time and 4ms write times. The drives must be Number required...(the required amount is 72GB) each. Mandatory for Blade Servers only is not being used for virtualization.	Y
30	Solution must support Internal hard drive speed with a minimum of 10K RPM. Mandatory for Blade Servers only is not being used for virtualization.	Y
31	Solution must support Internal hard drive capacity requirement with a minimum specified per Workload specific usable storage space for Rack Mount Servers.	450GB
32	The solution is required to support a minimum Controller Cache for internal storage of 512MB with battery backup.	Y
33	If there is a need for additional local storage, than Internal drives will be configured with the following RAID configuration on controller 2 provided (e.g. "temp file" for transaction or standalone server configurations). The additional drives may be required and will be configured with the appropriate RAID technology based on the application's performance and availability requirements. For any application that requires a database server the second controller is a requirement. Optimal configuration consists of the fewest quantity of drives in order to meet the performance and reliability requirements. The drives will be configured in the vendor's factory prior to delivery at the VA. RAID Configuration will be RAID1 for Rack Mount Servers. Not applicable for Blade Server.	Y
34	Solution BIOS must support boot from SAN	Y
35	Solution must be virtualization aware and capable of supporting Type 1 virtualization	Y
36	Solution must be configured with a minimum of N+1 redundancy for the cooling fan.	Y
37	External storage will be fibre channel/iSCSI/NFS/or determined by application requirements (specified at time of delivery order). If the connection is FC (fibre channel) the server must provide dual HBA FC cards with duplex LC connector. If using FC HBAs, the HBAs must provide load balancing and failover. If the connect is SCSI, the server must provide (2) PCI-E compatible SCSI cards (one card will be connected, one will be a cold spare). All external storage cards will be installed and configured in the vendor factory prior to arrival at a VA facility. if the external storage is NONE, the server will require internal storage only as defined above in requirement 10 (default is SCSI)	Y

38	Solution must consist of a minimum port count for External storage of 2 independent cards with a minimum of 2 ports each. For Rack Mount Servers only.	Y
39	Solution must consist of a minimum Bandwidth for External storage of 4GB for optical or 1GB for copper. Required number is 4GB for Optical and 1GB for Copper.	Y
40	Solution for External Storage must support storage interface devices in accordance to the task order. Solution must be supported by the Operating System specified within the task order.	Y
41	Solution for External storage for Blade Chassis Component must include Dual embedded switches. This also may require Blade Enclosure Chassis to include required components as per task order. Mandatory for Blade Servers, only for Legacy Blade Architectures.	N
42	Server must support USB v2.0 or higher	Y
43	Server power supplies must provide N+1 redundancy.	Y
44	Server voltage must be 208V input voltage on power supply.	Y
45	Server cord type must be IEC.	Y
46	SERVER must provide lights out / out of band management functionality to include command line and console access, secure IP-based remote management that complies with all VA security requirements as listed within the PWS and the ability to power off/on/reset the server remotely through the use of a dedicated network interface.	Y
47	Server must provide remote management capability for Virtual media (allows remote system's CD/DVD (or ISO file) to be mounted on the managed system during management connection.	Y
48	Server must provide remote management capability to include Virtual Console (keyboard/video/mouse usage).	Y
49	Server must provide remote management capability for Virtual Console Sharing	Y
50	Server must provide remote management capability for Virtual flash media support (allows remote system's flash memory storage device to be mounted on the managed system during management connection.	Y
51	System will provide Active Directory support integration.	Y
52	Server will provide hardware management software as an agent or agent-less SNMP agent	Y
53	Hardware events for the server will include exceptions, diagnostics and failures. Information will be exposed through SNMP with documented MIBs	Y
54	All server information collected will be available to be collected to an enterprise management framework. Server collection data structure must be ODBC / JDBC compliant in a manner that preserves data fields for the diagnostic information (e.g: date/time, error code, module, description, system identification, status and system configuration)	Y

Attachment D - Server Specifications

55	There will be no Operating System loaded on any purchased system unless otherwise specified within task order. Hardware is required to Support the latest version of both Windows and Linux Operating Systems. Hardware is required to support the latest stable kernel version of Operating System. If Hardware is purchased with or for Linux Operating Systems it is required to be 64-bit hardware.	Y
56	Support for Remote KVM Control will include Remote Keyboard/Video/Mouse Control with the ability to remotely connect to the server's external keyboard, video, and mouse ports through a networked KVM switch. Also, include Remote Power Disconnect with the ability to remotely disconnect/reconnect server to power source	Y
57	The existing KVM technology is IP.	Y
58	The server solution will include KVM connectors/dongles as per task order	Y

	Heavy Workload Server (Class A) - Blade	
	OEM & Model/Part Number:	
Reference Number	Requirement	Blade Server
1	Solution must provide x86 or x64 processor. The solution requires the minimum number of processor sockets on the server.	>=2
2	Solution must meet performance capacity with the minimum value within the SPEC INT_RATE_BASE 2006 benchmark test. This should be demonstrated via published benchmark results applicable to the specific server configuration.	>=300
3	Solution must support a minimum Socket Count of which meets the Performance Benchmark Standards (found in reference 2)	Y
4	Solution must support a core count at a minimal amount to meet the Performance Benchmark Standards. (found in reference 2)	Y
5	Solution requires the minimum cores per processor as specified in the SPEC Benchmark Standard. (found in reference 2)	Y
6	Solution must have minimal Socket Count due to licensing cost per socket, and have minimum count for performance/capacity	Y
7	Solution must have minimum Core count expected for performance / capacity, level is equal to quad-core. Any amount that meets the Performance Benchmark Standards is sufficient	Y
8	Solution requires at minimum, the following GB of RAM. RAM must be compatible with CPU and full error correction functionality to include ECC. All memory modules must be the same type and size. All memory must be installed in a manner to take full advantage of processor capabilities.	128GB
9	Solution requires that all memory channels must be symmetrically populated to achieve memory bandwidth of referenced performance benchmark	Y
10	Solution requires at minimum 25% of the provided DIMM slots to be unpopulated at time of delivery.	Y
11	The solution must support at minimum, the following sustainable throughput IOs per second.	375 IOPs
12	Rack Mounted Server should not exceed (4U) in size and fit in an "industry standard" 42U rack without special modifications to the rack and/or server. The server mount brackets should be "generic" for all types of 42U racks. Rail type: Tool-less square-hole sliding. Cable: Side-reversible for non-blade solutions.	N
13	Blade type:	Double slot full height blade server (max)

14	The solution must be a rack or blade (specified at time of delivery order) server. If Rack mounted server, the rail type will be tool-less square-holes (default is RACK)	Y
15	(1) Hard drive raid controller that will support at minimum RAID1 and “hot spare” automatic drive rebuild functionality for (at minimum) RAID1 for “Rack Mount Servers”. When server is configured as a transaction server, a separate RAID Controller or second channel on the same controller is required for the “temp file” RAID group. Must support SAS drives.	N
16	The solution must support RAID 1 for Blade Servers. Must support SAS drives.	Y
17	The solution is required to have a minimum Controller Cache of 256MB. Blade Servers are only mandatory if not being virtualized. If virtualized, they will be boot from SAN.	Y
18	The solution must support a minimum of 1 Controller.	Y
19	The solution must support a minimum private 32KB L1 instructional cache and private 32KB L1 data cache for each processor core. Minimum 256KB L2 cache per core. 6MB or greater shared L3 cache.	Y
20	The solution must support processors capable of Symmetrical multi processing.	Y
21	Solution must support at minimum the following number of network interface cards with TCP checksum offload functionality. for Windows only.	N
22	Solution must support a minimum network port count of 2. More may be required dependant on virtual infrastructure requirements (to be specified at time of delivery order), for Rack Mount Servers Only.	N
23	Solution must support a minimum of 1GB of Bandwith.	N
24	Solution must support dual imbedded switches for Blade Chassis components for Blade Servers.	N
25	For Virtual Environments only, solution must support a base set of 4 ports to be used for virtual guests, 1 for the console, 1 for the live migration. Additional may be required dependant on the profile of workload/application. For Rack Mount Servers Only.	N
26	Solution must support a base set of 2 ports or more for cluster interconnects dependant on cluster traffic. For Cluster Environments. Number required...(minimum is 2)	N
27	Solution must support embedded port count of one “card”, all interfaces used are spread across two “cards” (to include at least on add-on NIC). The goal is physical separation of the chipset / ASIC used on the redundant port, for each function. Support for “simple failover” (with a single IP address) and independent usage (with multiple IP addresses) is required.	N

28	Solution must provide a minimum of (3) internal hard drives with average throughput of 80 MB/s with no greater than 4ms latency. Drives must support 3ms read times and 4ms write times. In support of this solution, the drives must provide at minimum the application specific (provided at time of delivery order) usable disk space.	N
29	Solution for Blade Servers will consist of Number required...(the required amount is 2) Internal Hard Drives with an average throughput of 80MB/s with no greater than 4ms latency. Drives must support 3ms read time and 4ms write times. The drives must be Number required...(the required amount is 72GB) each. Mandatory for Blade Servers only is not being used for virtualization.	Y
30	Solution must support Internal hard drive speed with a minimum of 10K RPM. Mandatory for Blade Servers only is not being used for virtualization.	Y
31	Solution must support Internal hard drive capacity requirement with a minimum specified per Workload specific usable storage space for Rack Mount Servers.	N
32	The solution is required to support a minimum Controller Cache for internal storage of 512MB with battery backup.	N
33	If there is a need for additional local storage, than Internal drives will be configured with the following RAID configuration on controller 2 provided (e.g. "temp file" for transaction or standalone server configurations). The additional drives may be required and will be configured with the appropriate RAID technology based on the application's performance and availability requirements. For any application that requires a database server the second controller is a requirement. Optimal configuration consists of the fewest quantity of drives in order to meet the performance and reliability requirements. The drives will be configured in the vendor's factory prior to delivery at the VA. RAID Configuration will be RAID1 for Rack Mount Servers. Not applicable for Blade Server.	N
34	Solution BIOS must support boot from SAN	Y
35	Solution must be virtualization aware and capable of supporting Type 1 virtualization	Y
36	Solution must be configured with a minimum of N+1 redundancy for the cooling fan.	Y
37	External storage will be fibre channel/iSCSI/NFS/or determined by application requirements (specified at time of delivery order). If the connection is FC (fibre channel) the server must provide dual HBA FC cards with duplex LC connector. If using FC HBAs, the HBAs must provide load balancing and failover. If the connect is SCSI, the server must provide (2) PCI-E compatible SCSI cards (one card will be connected, one will be a cold spare). All external storage cards will be installed and configured in the vendor factory prior to arrival at a VA facility. if the external storage is NONE, the server will require internal storage only as defined above in requirement 10 (default is SCSI)	N

38	Solution must consist of a minimum port count for External storage of 2 independent cards with a minimum of 2 ports each. For Rack Mount Servers only.	N
39	Solution must consist of a minimum Bandwidth for External storage of 4GB for optical or 1GB for copper. Required number is 4GB for Optical and 1GB for Copper.	N
40	Solution for External Storage must support storage interface devices in accordance to the task order. Solution must be supported by the Operating System specified within the task order.	N
41	Solution for External storage for Blade Chassis Component must include Dual embedded switches. This also may require Blade Enclosure Chassis to include required components as per task order. Mandatory for Blade Servers, only for Legacy Blade Architectures.	Y
42	Server must support USB v2.0 or higher	Y
43	Server power supplies must provide N+1 redundancy.	Y
44	Server voltage must be 208V input voltage on power supply.	Y
45	Server cord type must be IEC.	Y
46	SERVER must provide lights out / out of band management functionality to include command line and console access, secure IP-based remote management that complies with all VA security requirements as listed within the PWS and the ability to power off/on/reset the server remotely through the use of a dedicated network interface.	Y
47	Server must provide remote management capability for Virtual media (allows remote system's CD/DVD (or ISO file) to be mounted on the managed system during management connection.	Y
48	Server must provide remote management capability to include Virtual Console (keyboard/video/mouse usage).	Y
49	Server must provide remote management capability for Virtual Console Sharing	Y
50	Server must provide remote management capability for Virtual flash media support (allows remote system's flash memory storage device to be mounted on the managed system during management connection.	Y
51	System will provide Active Directory support integration.	Y
52	Server will provide hardware management software as an agent or agent-less SNMP agent	Y
53	Hardware events for the server will include exceptions, diagnostics and failures. Information will be exposed through SNMP with documented MIBs	Y
54	All server information collected will be available to be collected to an enterprise management framework. Server collection data structure must be ODBC / JDBC compliant in a manner that preserves data fields for the diagnostic information (e.g: date/time, error code, module, description, system identification, status and system configuration)	Y

Attachment D - Server Specifications

55	There will be no Operating System loaded on any purchased system unless otherwise specified within task order. Hardware is required to Support the latest version of both Windows and Linux Operating Systems. Hardware is required to support the latest stable kernel version of Operating System. If Hardware is purchased with or for Linux Operating Systems it is required to be 64-bit hardware.	Y
56	Support for Remote KVM Control will include Remote Keyboard/Video/Mouse Control with the ability to remotely connect to the server's external keyboard, video, and mouse ports through a networked KVM switch. Also, include Remote Power Disconnect with the ability to remotely disconnect/reconnect server to power source	Y
57	The existing KVM technology is IP.	Y
58	The server solution will include KVM connectors/dongles as per task order	Y

	Medium Workload Server (Class B) - Rack	
	OEM & Model/Part Number:	
Reference Number	Requirement	Rack Mount Server
1	Solution must provide x86 or x64 processor. The solution requires the minimum number of processor sockets on the server.	>=2
2	Solution must meet performance capacity with the minimum value within the SPEC INT_RATE_BASE 2006 benchmark test. This should be demonstrated via published benchmark results applicable to the specific server configuration.	>=200
3	Solution must support a minimum Socket Count of which meets the Performance Benchmark Standards (found in reference 2)	Y
4	Solution must support a core count at a minimal amount to meet the Performance Benchmark Standards. (found in reference 2)	Y
5	Solution requires the minimum cores per processor as specified in the SPEC Benchmark Standard. (found in reference 2)	Y
6	Solution must have minimal Socket Count due to licensing cost per socket, and have minimum count for performance/capacity	Y
7	Solution must have minimum Core count expected for performance / capacity, level is equal to quad-core. Any amount that meets the Performance Benchmark Standards is sufficient	Y
8	Solution requires at minimum, the following GB of RAM. RAM must be compatible with CPU and full error correction functionality to include ECC. All memory modules must be the same type and size. All memory must be installed in a manner to take full advantage of processor capabilities.	48GB
9	Solution requires that all memory channels must be symmetrically populated to achieve memory bandwidth of referenced performance benchmark	Y
10	Solution requires at minimum 25% of the provided DIMM slots to be unpopulated at time of delivery.	Y
11	The solution must support at minimum, the following sustainable throughput IOs per second.	150 IOPs
12	Rack Mounted Server should not exceed (2U) in size and fit in an "industry standard" 42U rack without special modifications to the rack and/or server. The server mount brackets should be "generic" for all types of 42U racks. Rail type: Tool-less square-hole sliding. Cable: Side-reversible for non-blade solutions.	Y
13	Rack mount type	2U

14	The solution must be a rack or blade (specified at time of delivery order) server. If Rack mounted server, the rail type will be tool-less square-holes (default is RACK)	Y
15	(1) Hard drive raid controller that will support at minimum RAID1 and "hot spare" automatic drive rebuild functionality for (at minimum) RAID1 for "Rack Mount Servers". When server is configured as a transaction server, a separate RAID Controller or second channel on the same controller is required for the "temp file" RAID group. Must support SAS drives.	Y
16	The solution must support RAID 1 for Blade Servers. Must support SAS drives.	N
17	The solution is required to have a minimum Controller Cache of 256MB. Blade Servers are only mandatory if not being virtualized. If virtualized, they will be boot from SAN.	Y
18	The solution must support a minimum of 1 Controller.	Y
19	The solution must support a minimum private 32KB L1 instructional cache and private 32KB L1 data cache for each processor core. Minimum 256KB L2 cache per core. 6MB or greater shared L3 cache.	Y
20	The solution must support processors capable of Symmetrical multi processing.	Y
21	Solution must support at minimum the following number of network interface cards with TCP checksum offload functionality. for Windows only.	2
22	Solution must support a minimum network port count of 2. More may be required dependant on virtual infrastructure requirements (to be specified at time of delivery order), for Rack Mount Servers Only.	Y
23	Solution must support a minimum of 1GB of Bandwidth.	Y
24	Solution must support dual imbedded switches for Blade Chassis components for Blade Servers.	N
25	For Virtual Environments only, solution must support a base set of 4 ports to be used for virtual guests, 1 for the console, 1 for the live migration. Additional may be required dependant on the profile of workload/application. For Rack Mount Servers Only.	Y
26	Solution must support a base set of 2 ports or more for cluster interconnects dependant on cluster traffic. For Cluster Environments. Number required...(minimum is 2)	Y
27	Solution must support embedded port count of one "card", all interfaces used are spread across two "cards" (to include at least on add-on NIC). The goal is physical separation of the chipset / ASIC used on the redundant port, for each function. Support for "simple failover" (with a single IP address) and independent usage (with multiple IP addresses) is required.	Y

28	Solution must provide a minimum of (3) internal hard drives with average throughput of 80 MB/s with no greater than 4ms latency. Drives must support 3ms read times and 4ms write times. In support of this solution, the drives must provide at minimum the application specific (provided at time of delivery order) usable disk space.	Y
29	Solution for Blade Servers will consist of Number required...(the required amount is 2) Internal Hard Drives with an average throughput of 80MB/s with no greater than 4ms latency. Drives must support 3ms read time and 4ms write times. The drives must be Number required...(the required amount is 72GB) each. Mandatory for Blade Servers only is not being used for virtualization.	Y
30	Solution must support Internal hard drive speed with a minimum of 10K RPM. Mandatory for Blade Servers only is not being used for virtualization.	Y
31	Solution must support Internal hard drive capacity requirement with a minimum specified per Workload specific usable storage space for Rack Mount Servers.	300GB
32	The solution is required to support a minimum Controller Cache for internal stoage of 512MB with battery backup.	Y
33	If there is a need for additional local storage, than Internal drives will be configured with the following RAID configuration on controller 2 provided (e.g. "temp file" for transaction or standalone server configurations). The additional drives may be required and will be configured with the appropriate RAID technology based on the application's performance and availability requirements. For any application that requires a database server the second controller is a requirement. Optimal configuration consists of the fewest quantity of drives in order to meet the performance and reliability requirements. The drives will be configured in the vendor's factory prior to delivery at the VA. RAID Configuration will be RAID1 for Rack Mount Servers. Not applicable for Blade Server.	Y
34	Solution BIOS must support boot from SAN	Y
35	Solution must be virtualization aware and capable of supporting Type 1 virtualization	Y
36	Solution must be configured with a minimum of N+1 redundancy for the cooling fan.	Y
37	External storage will be fibre channel/iSCSI/NFS/or determined by application requirements (specified at time of delivery order). If the connection is FC (fibre channel) the server must provide dual HBA FC cards with duplex LC connector. If using FC HBAs, the HBAs must provide load balancing and failover. If the connect is SCSI, the server must provide (2) PCI-E compatible SCSI cards (one card will be connected, one will be a cold spare). All external storage cards will be installed and configured in the vendor factory prior to arrival at a VA facility. if the external storage is NONE, the server will require internal storage only as defined above in requirement 10 (default is SCSI)	Y

38	Solution must consist of a minimum port count for External storage of 2 independent cards with a minimum of 2 ports each. For Rack Mount Servers only.	Y
39	Solution must consist of a minimum Bandwidth for External storage of 4GB for optical or 1GB for copper. Required number is 4GB for Optical and 1GB for Copper.	Y
40	Solution for External Storage must support storage interface devices in accordance to the task order. Solution must be supported by the Operating System specified within the task order.	Y
41	Solution for External storage for Blade Chassis Component must include Dual embedded switches. This also may require Blade Enclosure Chassis to include required components as per task order. Mandatory for Blade Servers, only for Legacy Blade Architectures.	N
42	Server must support USB v2.0 or higher	Y
43	Server power supplies must provide N+1 redundancy.	Y
44	Server voltage must be 208V input voltage on power supply.	Y
45	Server cord type must be IEC.	Y
46	SERVER must provide lights out / out of band management functionality to include command line and console access, secure IP-based remote management that complies with all VA security requirements as listed within the PWS and the ability to power off/on/reset the server remotely through the use of a dedicated network interface.	Y
47	Server must provide remote management capability for Virtual media (allows remote system's CD/DVD (or ISO file) to be mounted on the managed system during management connection.	Y
48	Server must provide remote management capability to include Virtual Console (keyboard/video/mouse usage).	Y
49	Server must provide remote management capability for Virtual Console Sharing	Y
50	Server must provide remote management capability for Virtual flash media support (allows remote system's flash memory storage device to be mounted on the managed system during management connection.	Y
51	System will provide Active Directory support integration.	Y
52	Server will provide hardware management software as an agent or agent-less SNMP agent	Y
53	Hardware events for the server will include exceptions, diagnostics and failures. Information will be exposed through SNMP with documented MIBs	Y
54	All server information collected will be available to be collected to an enterprise management framework. Server collection data structure must be ODBC / JDBC compliant in a manner that preserves data fields for the diagnostic information (e.g: date/time, error code, module, description, system identification, status and system configuration)	Y

Attachment D - Server Specifications

55	There will be no Operating System loaded on any purchased system unless otherwise specified within task order. Hardware is required to Support the latest version of both Windows and Linux Operating Systems. Hardware is required to support the latest stable kernel version of Operating System. If Hardware is purchased with or for Linux Operating Systems it is required to be 64-bit hardware.	Y
56	Support for Remote KVM Control will include Remote Keyboard/Video/Mouse Control with the ability to remotely connect to the server's external keyboard, video, and mouse ports through a networked KVM switch. Also, include Remote Power Disconnect with the ability to remotely disconnect/reconnect server to power source	Y
57	The existing KVM technology is IP.	Y
58	The server solution will include KVM connectors/dongles as per task order	Y

	Medium Workload Server (Class B) - Blade	
	OEM & Model/Part Number:	
Reference Number	Requirement	Blade Server
1	Solution must provide x86 or x64 processor. The solution requires the minimum number of processor sockets on the server.	≥ 2
2	Solution must meet performance capacity with the minimum value within the SPEC INT_RATE_BASE 2006 benchmark test. This should be demonstrated via published benchmark results applicable to the specific server configuration.	≥ 200
3	Solution must support a minimum Socket Count of which meets the Performance Benchmark Standards (found in reference 2)	Y
4	Solution must support a core count at a minimal amount to meet the Performance Benchmark Standards. (found in reference 2)	Y
5	Solution requires the minimum cores per processor as specified in the SPEC Benchmark Standard. (found in reference 2)	Y
6	Solution must have minimal Socket Count due to licensing cost per socket, and have minimum count for performance/capacity	Y
7	Solution must have minimum Core count expected for performance / capacity, level is equal to quad-core. Any amount that meets the Performance Benchmark Standards is sufficient	Y
8	Solution requires at minimum, the following GB of RAM. RAM must be compatible with CPU and full error correction functionality to include ECC. All memory modules must be the same type and size. All memory must be installed in a manner to take full advantage of processor capabilities.	48GB
9	Solution requires that all memory channels must be symmetrically populated to achieve memory bandwidth of referenced performance benchmark	Y
10	Solution requires at minimum 25% of the provided DIMM slots to be unpopulated at time of delivery.	Y
11	The solution must support at minimum, the following sustainable throughput IOs per second.	150 IOPs
12	Rack Mounted Server should not exceed (2U) in size and fit in an "industry standard" 42U rack without special modifications to the rack and/or server. The server mount brackets should be "generic" for all types of 42U racks. Rail type: Tool-less square-hole sliding. Cable: Side-reversible for non-blade solutions.	N
13	Blade type	Double slot full height blade server (max)

14	The solution must be a rack or blade (specified at time of delivery order) server. If Rack mounted server, the rail type will be tool-less square-holes (default is RACK)	Y
15	(1) Hard drive raid controller that will support at minimum RAID1 and “hot spare” automatic drive rebuild functionality for (at minimum) RAID1 for “Rack Mount Servers”. When server is configured as a transaction server, a separate RAID Controller or second channel on the same controller is required for the “temp file” RAID group. Must support SAS drives.	N
16	The solution must support RAID 1 for Blade Servers. Must support SAS drives.	Y
17	The solution is required to have a minimum Controller Cache of 256MB. Blade Servers are only mandatory if not being virtualized. If virtualized, they will be boot from SAN.	Y
18	The solution must support a minimum of 1 Controller.	Y
19	The solution must support a minimum private 32KB L1 instructional cache and private 32KB L1 data cache for each processor core. Minimum 256KB L2 cache per core. 6MB or greater shared L3 cache.	Y
20	The solution must support processors capable of Symmetrical multi processing.	Y
21	Solution must support at minimum the following number of network interface cards with TCP checksum offload functionality. for Windows only.	N
22	Solution must support a minimum network port count of 2. More may be required dependant on virtual infrastructure requirements (to be specified at time of delivery order), for Rack Mount Servers Only.	N
23	Solution must support a minimum of 1GB of Bandwith.	N
24	Solution must support dual imbedded switches for Blade Chassis components for Blade Servers.	N
25	For Virtual Environments only, solution must support a base set of 4 ports to be used for virtual guests, 1 for the console, 1 for the live migration. Additional may be required dependant on the profile of workload/application. For Rack Mount Servers Only.	N
26	Solution must support a base set of 2 ports or more for cluster interconnects dependant on cluster traffic. For Cluster Environments. Number required...(minimum is 2)	N
27	Solution must support embedded port count of one “card”, all interfaces used are spread across two “cards” (to include at least on add-on NIC). The goal is physical separation of the chipset / ASIC used on the redundant port, for each function. Support for “simple failover” (with a single IP address) and independent usage (with multiple IP addresses) is required.	N

28	Solution must provide a minimum of (3) internal hard drives with average throughput of 80 MB/s with no greater than 4ms latency. Drives must support 3ms read times and 4ms write times. In support of this solution, the drives must provide at minimum the application specific (provided at time of delivery order) usable disk space.	N
29	Solution for Blade Servers will consist of Number required...(the required amount is 2) Internal Hard Drives with an average throughput of 80MB/s with no greater than 4ms latency. Drives must support 3ms read time and 4ms write times. The drives must be Number required...(the required amount is 72GB) each. Mandatory for Blade Servers only is not being used for virtualization.	Y
30	Solution must support Internal hard drive speed with a minimum of 10K RPM. Mandatory for Blade Servers only is not being used for virtualization.	Y
31	Solution must support Internal hard drive capacity requirement with a minimum specified per Workload specific usable storage space for Rack Mount Servers.	N
32	The solution is required to support a minimum Controller Cache for internal storage of 512MB with battery backup.	N
33	If there is a need for additional local storage, than Internal drives will be configured with the following RAID configuration on controller 2 provided (e.g. "temp file" for transaction or standalone server configurations). The additional drives may be required and will be configured with the appropriate RAID technology based on the application's performance and availability requirements. For any application that requires a database server the second controller is a requirement. Optimal configuration consists of the fewest quantity of drives in order to meet the performance and reliability requirements. The drives will be configured in the vendor's factory prior to delivery at the VA. RAID Configuration will be RAID1 for Rack Mount Servers. Not applicable for Blade Server.	N
34	Solution BIOS must support boot from SAN	Y
35	Solution must be virtualization aware and capable of supporting Type 1 virtualization	Y
36	Solution must be configured with a minimum of N+1 redundancy for the cooling fan.	Y
37	External storage will be fibre channel/iSCSI/NFS/or determined by application requirements (specified at time of delivery order). If the connection is FC (fibre channel) the server must provide dual HBA FC cards with duplex LC connector. If using FC HBAs, the HBAs must provide load balancing and failover. If the connect is SCSI, the server must provide (2) PCI-E compatible SCSI cards (one card will be connected, one will be a cold spare). All external storage cards will be installed and configured in the vendor factory prior to arrival at a VA facility. if the external storage is NONE, the server will require internal storage only as defined above in requirement 10 (default is SCSI)	N

38	Solution must consist of a minimum port count for External storage of 2 independent cards with a minimum of 2 ports each. For Rack Mount Servers only.	N
39	Solution must consist of a minimum Bandwidth for External storage of 4GB for optical or 1GB for copper. Required number is 4GB for Optical and 1GB for Copper.	N
40	Solution for External Storage must support storage interface devices in accordance to the task order. Solution must be supported by the Operating System specified within the task order.	N
41	Solution for External storage for Blade Chassis Component must include Dual embedded switches. This also may require Blade Enclosure Chassis to include required components as per task order. Mandatory for Blade Servers, only for Legacy Blade Architectures.	Y
42	Server must support USB v2.0 or higher	Y
43	Server power supplies must provide N+1 redundancy.	Y
44	Server voltage must be 208V input voltage on power supply.	Y
45	Server cord type must be IEC.	Y
46	SERVER must provide lights out / out of band management functionality to include command line and console access, secure IP-based remote management that complies with all VA security requirements as listed within the PWS and the ability to power off/on/reset the server remotely through the use of a dedicated network interface.	Y
47	Server must provide remote management capability for Virtual media (allows remote system's CD/DVD (or ISO file) to be mounted on the managed system during management connection.	Y
48	Server must provide remote management capability to include Virtual Console (keyboard/video/mouse usage).	Y
49	Server must provide remote management capability for Virtual Console Sharing	Y
50	Server must provide remote management capability for Virtual flash media support (allows remote system's flash memory storage device to be mounted on the managed system during management connection.	Y
51	System will provide Active Directory support integration.	Y
52	Server will provide hardware management software as an agent or agent-less SNMP agent	Y
53	Hardware events for the server will include exceptions, diagnostics and failures. Information will be exposed through SNMP with documented MIBs	Y
54	All server information collected will be available to be collected to an enterprise management framework. Server collection data structure must be ODBC / JDBC compliant in a manner that preserves data fields for the diagnostic information (e.g: date/time, error code, module, description, system identification, status and system configuration)	Y

Attachment D - Server Specifications

55	There will be no Operating System loaded on any purchased system unless otherwise specified within task order. Hardware is required to Support the latest version of both Windows and Linux Operating Systems. Hardware is required to support the latest stable kernel version of Operating System. If Hardware is purchased with or for Linux Operating Systems it is required to be 64-bit hardware.	Y
56	Support for Remote KVM Control will include Remote Keyboard/Video/Mouse Control with the ability to remotely connect to the server's external keyboard, video, and mouse ports through a networked KVM switch. Also, include Remote Power Disconnect with the ability to remotely disconnect/reconnect server to power source	Y
57	The existing KVM technology is IP.	Y
58	The server solution will include KVM connectors/dongles as per task order	Y

	Light Workload Server (Class C) - Rack	
	OEM & Model/Part Number:	
Reference Number	Requirement	Rack Mount Server
1	Solution must provide x86 or x64 processor. The solution requires the minimum number of processor sockets on the server.	>=1
2	Solution must meet performance capacity with the minimum value within the SPEC INT_RATE_BASE 2006 benchmark test. This should be demonstrated via published benchmark results applicable to the specific server configuration.	>=200
3	Solution must support a minimum Socket Count of which meets the Performance Benchmark Standards (found in reference 2)	Y
4	Solution must support a core count at a minimal amount to meet the Performance Benchmark Standards. (found in reference 2)	Y
5	Solution requires the minimum cores per processor as specified in the SPEC Benchmark Standard. (found in reference 2)	Y
6	Solution must have minimal Socket Count due to licensing cost per socket, and have minimum count for performance/capacity	Y
7	Solution must have minimum Core count expected for performance / capacity, level is equal to quad-core. Any amount that meets the Performance Benchmark Standards is sufficient	Y
8	Solution requires at minimum, the following GB of RAM. RAM must be compatible with CPU and full error correction functionality to include ECC. All memory modules must be the same type and size. All memory must be installed in a manner to take full advantage of processor capabilities.	16GB
9	Solution requires that all memory channels must be symmetrically populated to achieve memory bandwidth of referenced performance benchmark	Y
10	Solution requires at minimum 25% of the provided DIMM slots to be unpopulated at time of delivery.	Y
11	The solution must support at minimum, the following sustainable throughput IOs per second.	75 IOPs
12	Rack Mounted Server should not exceed (2U) in size and fit in an "industry standard" 42U rack without special modifications to the rack and/or server. The server mount brackets should be "generic" for all types of 42U racks. Rail type: Tool-less square-hole sliding. Cable: Side-reversible for non-blade solutions.	Y
13	Rack mount type	2U

14	The solution must be a rack or blade (specified at time of delivery order) server. If Rack mounted server, the rail type will be tool-less square-holes (default is RACK)	Y
15	(1) Hard drive raid controller that will support at minimum RAID1 and "hot spare" automatic drive rebuild functionality for (at minimum) RAID1 for "Rack Mount Servers". When server is configured as a transaction server, a separate RAID Controller or second channel on the same controller is required for the "temp file" RAID group. Must support SAS drives.	Y
16	The solution must support RAID 1 for Blade Servers. Must support SAS drives.	N
17	The solution is required to have a minimum Controller Cache of 256MB. Blade Servers are only mandatory if not being virtualized. If virtualized, they will be boot from SAN.	Y
18	The solution must support a minimum of 1 Controller.	Y
19	The solution must support a minimum private 32KB L1 instructional cache and private 32KB L1 data cache for each processor core. Minimum 256KB L2 cache per core. 6MB or greater shared L3 cache.	Y
20	The solution must support processors capable of Symmetrical multi processing.	Y
21	Solution must support at minimum the following number of network interface cards with TCP checksum offload functionality. for Windows only.	2
22	Solution must support a minimum network port count of 2. More may be required dependant on virtual infrastructure requirements (to be specified at time of delivery order), for Rack Mount Servers Only.	Y
23	Solution must support a minimum of 1GB of Bandwidth.	Y
24	Solution must support dual imbedded switches for Blade Chassis components for Blade Servers.	N
25	For Virtual Environments only, solution must support a base set of 4 ports to be used for virtual guests, 1 for the console, 1 for the live migration. Additional may be required dependant on the profile of workload/application. For Rack Mount Servers Only.	Y
26	Solution must support a base set of 2 ports or more for cluster interconnects dependant on cluster traffic. For Cluster Environments. Number required...(minimum is 2)	Y
27	Solution must support embedded port count of one "card", all interfaces used are spread across two "cards" (to include at least on add-on NIC). The goal is physical separation of the chipset / ASIC used on the redundant port, for each function. Support for "simple failover" (with a single IP address) and independent usage (with multiple IP addresses) is required.	Y

28	Solution must provide a minimum of (3) internal hard drives with average throughput of 80 MB/s with no greater than 4ms latency. Drives must support 3ms read times and 4ms write times. In support of this solution, the drives must provide at minimum the application specific (provided at time of delivery order) usable disk space.	Y
29	Solution for Blade Servers will consist of Number required...(the required amount is 2) Internal Hard Drives with an average throughput of 80MB/s with no greater than 4ms latency. Drives must support 3ms read time and 4ms write times. The drives must be Number required...(the required amount is 72GB) each. Mandatory for Blade Servers only is not being used for virtualization.	Y
30	Solution must support Internal hard drive speed with a minimum of 10K RPM. Mandatory for Blade Servers only is not being used for virtualization.	Y
31	Solution must support Internal hard drive capacity requirement with a minimum specified per Workload specific usable storage space for Rack Mount Servers.	72GB
32	The solution is required to support a minimum Controller Cache for internal stoage of 512MB with battery backup.	Y
33	If there is a need for additional local storage, than Internal drives will be configured with the following RAID configuration on controller 2 provided (e.g. "temp file" for transaction or standalone server configurations). The additional drives may be required and will be configured with the appropriate RAID technology based on the application's performance and availability requirements. For any application that requires a database server the second controller is a requirement. Optimal configuration consists of the fewest quantity of drives in order to meet the performance and reliability requirements. The drives will be configured in the vendor's factory prior to delivery at the VA. RAID Configuration will be RAID1 for Rack Mount Servers. Not applicable for Blade Server.	Y
34	Solution BIOS must support boot from SAN	Y
35	Solution must be virtualization aware and capable of supporting Type 1 virtualization	Y
36	Solution must be configured with a minimum of N+1 redundancy for the cooling fan.	Y
37	External storage will be fibre channel/iSCSI/NFS/or determined by application requirements (specified at time of delivery order). If the connection is FC (fibre channel) the server must provide dual HBA FC cards with duplex LC connector. If using FC HBAs, the HBAs must provide load balancing and failover. If the connect is SCSI, the server must provide (2) PCI-E compatible SCSI cards (one card will be connected, one will be a cold spare). All external storage cards will be installed and configured in the vendor factory prior to arrival at a VA facility. if the external storage is NONE, the server will require internal storage only as defined above in requirement 10 (default is SCSI)	Y

38	Solution must consist of a minimum port count for External storage of 2 independent cards with a minimum of 2 ports each. For Rack Mount Servers only.	Y
39	Solution must consist of a minimum Bandwidth for External storage of 4GB for optical or 1GB for copper. Required number is 4GB for Optical and 1GB for Copper.	Y
40	Solution for External Storage must support storage interface devices in accordance to the task order. Solution must be supported by the Operating System specified within the task order.	Y
41	Solution for External storage for Blade Chassis Component must include Dual embedded switches. This also may require Blade Enclosure Chassis to include required components as per task order. Mandatory for Blade Servers, only for Legacy Blade Architectures.	N
42	Server must support USB v2.0 or higher	Y
43	Server power supplies must provide N+1 redundancy.	Y
44	Server voltage must be 208V input voltage on power supply.	Y
45	Server cord type must be IEC.	Y
46	SERVER must provide lights out / out of band management functionality to include command line and console access, secure IP-based remote management that complies with all VA security requirements as listed within the PWS and the ability to power off/on/reset the server remotely through the use of a dedicated network interface.	Y
47	Server must provide remote management capability for Virtual media (allows remote system's CD/DVD (or ISO file) to be mounted on the managed system during management connection.	Y
48	Server must provide remote management capability to include Virtual Console (keyboard/video/mouse usage).	Y
49	Server must provide remote management capability for Virtual Console Sharing	Y
50	Server must provide remote management capability for Virtual flash media support (allows remote system's flash memory storage device to be mounted on the managed system during management connection.	Y
51	System will provide Active Directory support integration.	Y
52	Server will provide hardware management software as an agent or agent-less SNMP agent	Y
53	Hardware events for the server will include exceptions, diagnostics and failures. Information will be exposed through SNMP with documented MIBs	Y
54	All server information collected will be available to be collected to an enterprise management framework. Server collection data structure must be ODBC / JDBC compliant in a manner that preserves data fields for the diagnostic information (e.g: date/time, error code, module, description, system identification, status and system configuration)	Y

Attachment D - Server Specifications

55	There will be no Operating System loaded on any purchased system unless otherwise specified within task order. Hardware is required to Support the latest version of both Windows and Linux Operating Systems. Hardware is required to support the latest stable kernel version of Operating System. If Hardware is purchased with or for Linux Operating Systems it is required to be 64-bit hardware.	Y
56	Support for Remote KVM Control will include Remote Keyboard/Video/Mouse Control with the ability to remotely connect to the server's external keyboard, video, and mouse ports through a networked KVM switch. Also, include Remote Power Disconnect with the ability to remotely disconnect/reconnect server to power source	Y
57	The existing KVM technology is IP.	Y
58	The server solution will include KVM connectors/dongles as per task order	Y

	Light Workload Server (Class C) - Blade	
	OEM & Model/Part Number:	
Reference Number	Requirement	Blade Server
1	Solution must provide x86 or x64 processor. The solution requires the minimum number of processor sockets on the server.	>=1
2	Solution must meet performance capacity with the minimum value within the SPEC INT_RATE_BASE 2006 benchmark test. This should be demonstrated via published benchmark results applicable to the specific server configuration.	>=200
3	Solution must support a minimum Socket Count of which meets the Performance Benchmark Standards (found in reference 2)	Y
4	Solution must support a core count at a minimal amount to meet the Performance Benchmark Standards. (found in reference 2)	Y
5	Solution requires the minimum cores per processor as specified in the SPEC Benchmark Standard. (found in reference 2)	Y
6	Solution must have minimal Socket Count due to licensing cost per socket, and have minimum count for performance/capacity	Y
7	Solution must have minimum Core count expected for performance / capacity, level is equal to quad-core. Any amount that meets the Performance Benchmark Standards is sufficient	Y
8	Solution requires at minimum, the following GB of RAM. RAM must be compatible with CPU and full error correction functionality to include ECC. All memory modules must be the same type and size. All memory must be installed in a manner to take full advantage of processor capabilities.	16GB
9	Solution requires that all memory channels must be symmetrically populated to achieve memory bandwidth of referenced performance benchmark	Y
10	Solution requires at minimum 25% of the provided DIMM slots to be unpopulated at time of delivery.	Y
11	The solution must support at minimum, the following sustainable throughput IOs per second.	75 IOPs
12	Rack Mounted Server should not exceed (2U) in size and fit in an "industry standard" 42U rack without special modifications to the rack and/or server. The server mount brackets should be "generic" for all types of 42U racks. Rail type: Tool-less square-hole sliding. Cable: Side-reversible for non-blade solutions.	N
13	Blade type	Double slot full height blade server (max)

14	The solution must be a rack or blade (specified at time of delivery order) server. If Rack mounted server, the rail type will be tool-less square-holes (default is RACK)	Y
15	(1) Hard drive raid controller that will support at minimum RAID1 and “hot spare” automatic drive rebuild functionality for (at minimum) RAID1 for “Rack Mount Servers”. When server is configured as a transaction server, a separate RAID Controller or second channel on the same controller is required for the “temp file” RAID group. Must support SAS drives.	N
16	The solution must support RAID 1 for Blade Servers. Must support SAS drives.	Y
17	The solution is required to have a minimum Controller Cache of 256MB. Blade Servers are only mandatory if not being virtualized. If virtualized, they will be boot from SAN.	Y
18	The solution must support a minimum of 1 Controller.	Y
19	The solution must support a minimum private 32KB L1 instructional cache and private 32KB L1 data cache for each processor core. Minimum 256KB L2 cache per core. 6MB or greater shared L3 cache.	Y
20	The solution must support processors capable of Symmetrical multi processing.	Y
21	Solution must support at minimum the following number of network interface cards with TCP checksum offload functionality. for Windows only.	N
22	Solution must support a minimum network port count of 2. More may be required dependant on virtual infrastructure requirements (to be specified at time of delivery order), for Rack Mount Servers Only.	N
23	Solution must support a minimum of 1GB of Bandwith.	N
24	Solution must support dual imbedded switches for Blade Chassis components for Blade Servers.	N
25	For Virtual Environments only, solution must support a base set of 4 ports to be used for virtual guests, 1 for the console, 1 for the live migration. Additional may be required dependant on the profile of workload/application. For Rack Mount Servers Only.	N
26	Solution must support a base set of 2 ports or more for cluster interconnects dependant on cluster traffic. For Cluster Environments. Number required...(minimum is 2)	N
27	Solution must support embedded port count of one “card”, all interfaces used are spread across two “cards” (to include at least on add-on NIC). The goal is physical separation of the chipset / ASIC used on the redundant port, for each function. Support for “simple failover” (with a single IP address) and independent usage (with multiple IP addresses) is required.	N

28	Solution must provide a minimum of (3) internal hard drives with average throughput of 80 MB/s with no greater than 4ms latency. Drives must support 3ms read times and 4ms write times. In support of this solution, the drives must provide at minimum the application specific (provided at time of delivery order) usable disk space.	N
29	Solution for Blade Servers will consist of Number required...(the required amount is 2) Internal Hard Drives with an average throughput of 80MB/s with no greater than 4ms latency. Drives must support 3ms read time and 4ms write times. The drives must be Number required...(the required amount is 72GB) each. Mandatory for Blade Servers only is not being used for virtualization.	Y
30	Solution must support Internal hard drive speed with a minimum of 10K RPM. Mandatory for Blade Servers only is not being used for virtualization.	Y
31	Solution must support Internal hard drive capacity requirement with a minimum specified per Workload specific usable storage space for Rack Mount Servers.	N
32	The solution is required to support a minimum Controller Cache for internal storage of 512MB with battery backup.	N
33	If there is a need for additional local storage, than Internal drives will be configured with the following RAID configuration on controller 2 provided (e.g. "temp file" for transaction or standalone server configurations). The additional drives may be required and will be configured with the appropriate RAID technology based on the application's performance and availability requirements. For any application that requires a database server the second controller is a requirement. Optimal configuration consists of the fewest quantity of drives in order to meet the performance and reliability requirements. The drives will be configured in the vendor's factory prior to delivery at the VA. RAID Configuration will be RAID1 for Rack Mount Servers. Not applicable for Blade Server.	N
34	Solution BIOS must support boot from SAN	Y
35	Solution must be virtualization aware and capable of supporting Type 1 virtualization	Y
36	Solution must be configured with a minimum of N+1 redundancy for the cooling fan.	Y
37	External storage will be fibre channel/iSCSI/NFS/or determined by application requirements (specified at time of delivery order). If the connection is FC (fibre channel) the server must provide dual HBA FC cards with duplex LC connector. If using FC HBAs, the HBAs must provide load balancing and failover. If the connect is SCSI, the server must provide (2) PCI-E compatible SCSI cards (one card will be connected, one will be a cold spare). All external storage cards will be installed and configured in the vendor factory prior to arrival at a VA facility. if the external storage is NONE, the server will require internal storage only as defined above in requirement 10 (default is SCSI)	N

38	Solution must consist of a minimum port count for External storage of 2 independent cards with a minimum of 2 ports each. For Rack Mount Servers only.	N
39	Solution must consist of a minimum Bandwidth for External storage of 4GB for optical or 1GB for copper. Required number is 4GB for Optical and 1GB for Copper.	N
40	Solution for External Storage must support storage interface devices in accordance to the task order. Solution must be supported by the Operating System specified within the task order.	N
41	Solution for External storage for Blade Chassis Component must include Dual embedded switches. This also may require Blade Enclosure Chassis to include required components as per task order. Mandatory for Blade Servers, only for Legacy Blade Architectures.	Y
42	Server must support USB v2.0 or higher	Y
43	Server power supplies must provide N+1 redundancy.	Y
44	Server voltage must be 208V input voltage on power supply.	Y
45	Server cord type must be IEC.	Y
46	SERVER must provide lights out / out of band management functionality to include command line and console access, secure IP-based remote management that complies with all VA security requirements as listed within the PWS and the ability to power off/on/reset the server remotely through the use of a dedicated network interface.	Y
47	Server must provide remote management capability for Virtual media (allows remote system's CD/DVD (or ISO file) to be mounted on the managed system during management connection.	Y
48	Server must provide remote management capability to include Virtual Console (keyboard/video/mouse usage).	Y
49	Server must provide remote management capability for Virtual Console Sharing	Y
50	Server must provide remote management capability for Virtual flash media support (allows remote system's flash memory storage device to be mounted on the managed system during management connection.	Y
51	System will provide Active Directory support integration.	Y
52	Server will provide hardware management software as an agent or agent-less SNMP agent	Y
53	Hardware events for the server will include exceptions, diagnostics and failures. Information will be exposed through SNMP with documented MIBs	Y
54	All server information collected will be available to be collected to an enterprise management framework. Server collection data structure must be ODBC / JDBC compliant in a manner that preserves data fields for the diagnostic information (e.g: date/time, error code, module, description, system identification, status and system configuration)	Y

Attachment D - Server Specifications

55	There will be no Operating System loaded on any purchased system unless otherwise specified within task order. Hardware is required to Support the latest version of both Windows and Linux Operating Systems. Hardware is required to support the latest stable kernel version of Operating System. If Hardware is purchased with or for Linux Operating Systems it is required to be 64-bit hardware.	Y
56	Support for Remote KVM Control will include Remote Keyboard/Video/Mouse Control with the ability to remotely connect to the server's external keyboard, video, and mouse ports through a networked KVM switch. Also, include Remote Power Disconnect with the ability to remotely disconnect/reconnect server to power source	Y
57	The existing KVM technology is IP.	Y
58	The server solution will include KVM connectors/dongles as per task order	Y

Heavy Workload Blade Chassis (Class A)			
OEM & Model/Part Number:			
Reference Number	Requirement	Mandatory	Optional Feature, Not Mandatory
1	Solution must support device bays sufficient to support 8 half height or 4 full height server or storage blades and the ability to mix form factors within the same chassis.	Y	
2	Solution must support a minimum of 80 Gb per chassis.	Y	
3	Solution must support independent hot swappable power supplies of sufficient quantity to power a fully populated chassis if two power supply failures occur at the same time.	Y	
4	Solution must support single-phase power subsystem. It is optional to also support three-phase or a -48V DC power subsystem.	Y	
5	Solution must support hot swappable fans of sufficient quantity to maintain a fully populated chassis within designed temperature limits in the event of 2 simultaneous fan failures.	Y	
6	Solution must not exceed 10U in height per single chassis.	Y	
7	Blade Server Management Software - Must support the ability to manage more than one chassis from the same console - Must support two or more simultaneous users - Must support multiple authentication mechanisms including Active Directory - Must support the ability to connect a virtual CD-ROM drive to individual blades - Must support the ability to power on/off and reset blades individually - Must provide real time monitoring of operational environment including blade temperature, power consumption, and hard drives that have failed or are pending failure - Must provide KVM console access to each blade individually	Y	
8	Solution will support Role-based security locally and/or with LDAP directory services.	Y	
9	Solution will provide a Blade Management Solution for Configuration and administration purposes.	Y	
10	Solution must support one or more of the following SAN Connectivity requirements; 4Gb, 8Gb with redundancy.	Y	
11	Solution must support north-bound SAN connectivity with a minimum of 6-8 Gb FC Connectivity.	Y	
12	Solution must support one or more of the following; 3 Gb 8-port SAS 2.0, iSCSI, or FCOE	Y	
13	Support for the following Interconnects: Low-latency and up to 40Gbps bandwidth with management and switch module		Y

14	Solution must support the following network connectivity requirements; 1-GbE, 10-GbE, 8-GbE FC with redundancy.	Y	
15	Support for one of the optional Interconnect modules: be able to divide each 10 Gb network connection into four independent physical NIC server connections. Each NIC can be configured from 100 Mb up to 10 Gb. Provide a full set of Layer 2 switching and Layer 3 routing features, sixteen internal downlinks, five uplinks and two internal cross-connects in a single blade switch, Blade Switch, 10 Gb Ethernet Blade Switch, 1/10 Gb Ethernet Module, 1 Gb Ethernet pass Thru Module, Blade 8 Gb SAN Switch		Y
16	Solution must support one or more of the following Power Cord options:	LV Power Cords 100-120V AC C19/C20 Jumper Cords HV Power Cords 200-240V AC	

Light Workload Blade Chassis (Class B-C)			
OEM & Model/Part Number:			
Reference Number	Requirement	Mandatory	Optional Feature, Not Mandatory
1	Solution must support device bays sufficient to support 8 half height or 4 full height server or storage blades and the ability to mix form factors within the same chassis.	y	
2	Solution must support a minimum of 80 Gb per chassis.	y	
3	Solution must support independent hot swappable power supplies of sufficient quantity to power a fully populated chassis if two power supply failures occur at the same time.	y	
4	Solution must support single-phase power subsystem. It is optional to also support three-phase or a -48V DC power subsystem.	y	
5	Solution must support hot swappable fans of sufficient quantity to maintain a fully populated chassis within designed temperature limits in the event of 2 simultaneous fan failures.	y	
6	Solution must not exceed 10U in height per single chassis.	y	
7	Blade Server Management Software - Must support the ability to manage more than one chassis from the same console - Must support two or more simultaneous users - Must support multiple authentication mechanisms including Active Directory - Must support the ability to connect a virtual CD-ROM drive to individual blades - Must support the ability to power on/off and reset blades individually - Must provide real time monitoring of operational environment including blade temperature, power consumption, and hard drives that have failed or are pending failure - Must provide KVM console access to each blade individually	y	
8	Solution will support Role-based security locally and/or with LDAP directory services.	y	
9	Solution will provide a Blade Management Solution for Configuration and administration purposes.	y	
10	Solution must support one or more of the following SAN Connectivity requirements; 4Gb, 8Gb with redundancy.	y	
11	Solution must support north-bound SAN connectivity with a minimum of 6-8 Gb FC Connectivity.	y	
12	Solution must support one or more of the following; 3 Gb 8-port SAS 2.0, iSCSI, or FCOE	y	
13	Support for the following Interconnects: Low-latency and up to 40Gbps bandwidth with management and switch module		y

14	Solution must support the following network connectivity requirements; 1-GbE, 10-GbE, 8-GbE FC with redundancy.	Y	
15	Support for one of the optional Interconnect modules: be able to divide each 10 Gb network connection into four independent physical NIC server connections. Each NIC can be configured from 100 Mb up to 10 Gb. Provide a full set of Layer 2 switching and Layer 3 routing features, sixteen internal downlinks, five uplinks and two internal cross-connects in a single blade switch, Blade Switch, 10 Gb Ethernet Blade Switch, 1/10 Gb Ethernet Module, 1 Gb Ethernet pass Thru Module, Blade 8 Gb SAN Switch		Y
16	Solution must support one or more of the following Power Cord options:	LV Power Cords 100-120V AC 2m 15A C13/C20 Jumper Cords HV Power Cords 200-240V AC	

Modular LAN Campus Core Switch				
ID	Ref. No.	Primary Attribute	Secondary Attribute	Specification
1	1	Chassis	Type	Modular
	2		19 Inch Rack Mounting	Required
	3		Packet Processor Redundancy	Required (Online Insertion/Removal)
	4		Packet Processor	Layer-3 Switching: Non-Blocking Layer-2 Switching: Non-Blocking
	5		Control Plane Redundancy Support	Required
	6		Cooling Redundancy Support	Required
	7		Power Supply Redundancy Support (1:1) or (N+1)	Required
	8		Input Power Options	AC
	9		Online Insertion/Removal Hot-Pluggable	Required
	10		Multi-Chassis Link Aggregation	Required
2	1	Operating System Features	Protocols switched in hardware	IPv4, IPv6, IGMP Snooping, IPv6 MLD v1 & v2
	2		Layer 3 Protocols & Routing Features	- IPv4, IPv6, ICMP, OSPF, BGP - Virtual Router Redundancy Protocol (VRRP) - Routing Engine Fast failover - Switching load sharing configurable per packet or per session, and per session is configuration with L3 address and L4 ports - Protocol Independent Multicast (PIM) v1 & v2
	3		OSPF Requirements	- IPv4 Open Shortest Path First (OSPF) versions 2 - IPv6 Open Shortest Path First (OSPF) versions 3 - MD5 authentication - Configurable areas, ABRs, and ASBRs - Configurable area types: normal (LSAs 1-5), stubby (LSAs 1-4), totally stubby (LSAs 1-2), Not-So-Stubby Area (NSSA) (LSAs 1-4 & 7), and NSSA totally stubby (LSAs 1-2 & 7) - Configurable router ID - Configurable hello packet interval - Configurable router dead interval - Configurable priority for DR and BDR - Configurable per interface network types (P2P, broadcast, NBMA, and virtual links) - Configurable cost per interface - Configurable cost multiplier - Ability to redistribute static routes and other protocol routes using access lists and route maps
	4		BGPv4 Requirements	- Multiprotocol Border Gateway Protocol (BGP) for IPv4 and IPv6 - MD5 authentication - Use all standard attributes - Ability to enable or disable synchronization - Configurable local preference per neighbor - Configurable multi-exit discriminator (MED) per neighbor - Configurable standard and extended communities
	5		Required L2 Features	802.1q, Per-port broadcast, multicast, and unicast storm control, 802.3ad (LACP), Link-Layer Discover Protocol, Jumbo Ethernet Frames with MTU up to 9000 bytes

	6		Port Security	- 802.1x Support - MAC Authentication Bypass - Dynamic VLAN Assignment - Configurable number of MAC Addresses allowed per port - Configurable actions to take when violation occurs - Ability to configure MAC address or addresses allowed per port - Ability to learn and stick a MAC Address per port
	7		QoS Features	- 802.1p class-of-service(CoS) classification - Differentiated Services Code Point (DSCP) classification - Support ingress classification, policing, and marking per port - Support egress queuing/scheduling - 15,000 source and 15,000 destination QoS ACL entries (processed in hardware)
	8		Access Control Lists	- Access lists in hardware - Support for access lists source and destination L2 MAC address, Ethernet types, and SAPs - Support for access lists source and destination L3 addresses with masks and L4 port numbers - Support for prefix lists - Ability to apply L3 access list to L2 interfaces/ports - Ability to police (rate limit) per port, per port channel, per VLAN - 15,000 source and 15,000 destination ACL entries (processed in hardware)
	9		NTP Support	- Version 3 or greater Required - Configurable NTP Peer and Server Associations - Configurable NTP Authentication - Configurable NTP Access Restrictions - Configurable Source IP Address for NTP packets - Configurable Timezone/Offset - Configurable automatic recurring daylight savings time - Configurable per Interface
	10		Unidirectional Link failure Detection	Required
	11		802.1d Required Spanning Tree Features	- Must be able to disable spanning tree per port - Ability to transition immediately to forwarding state per port on edge ports with 802.1d/s/w - Ability to disable topology change notifications per port on edge ports with 802.1d/s/w - STP cost configurable per port (0 to 240) 802.1d & 802.1t - STP priority configurable per VLAN (0 to 61,440) 802.1d & 802.1t - Ability to prevent rogue bridges from becoming the STP root - Ability to prevent an alternate port or a root port from assuming a designated port role due to the absence of BPDUs. - Ability to configure STP edge ports to disable upon receiving a BPDU

	12		Network Management	- Centralized AAA w/ Role Based Authorization, Syslog, SNMP v2c, v3, SNMP Traps, SSH, Telnet, Radius or similar - Ability to disable telnet, ftp, http, https - IPv6 Support - Secure console port with roles based AAA authentication - Configurable Console & VTY timeout - Ability to define and apply IP access control lists to VTY sessions - Out of Band Ethernet Management Port -Optional - DNS support for resolution of user-defined device names
	13		SNMP Features	- Support for, SNMPv2C, & SNMPv3 - Support for traps that is an agent on the switch to send an unsolicited notifications to the SNMP manager for a configured event. - Configurable source IP address or interface for traps. - Supports both read-only (RO) and read-write (RW) community strings - Ability to restrict each community string to specific IP addresses independently - Ability to configure different SNMP versions for each SNMP manager - Support for multiple RO and RW community strings - Support for multiple SNMP profiles
	14		Port Mirroring or similar	Required
	15		Remote Port Mirroring or similar	Required
	16		Configuration File Management	TFTP, FTP
	17		Software Image Management	TFTP, FTP
	18		VLAN Support	>= 1000 VLAN's
	19		Data Traffic Rate Limiting	- Source and Destination IP - Layer 4 TCP and UDP - Source and Destination MAC
	20		VOIP Features	Configurable Voice-VLAN
	21		Message Logging Buffer	- Configurable log history size - Configurable logging severity - Configurable log message time stamps
3	1	Line-cards / Port Interfaces	Throughput to Backplane	Non-Blocking option available
	2		Port per ASIC (Oversubscription)	1:1 Option Available
	3		Interface Speed Options	- 10/100 Mbps Ethernet - 10/100/1000 Mbps Ethernet - 1 Gbps Ethernet - 10 Gbps Ethernet
	4		Media Flexibility Options	MMF >= 220m, SMF >= 10km, IEEE 802.3z-compliant 1000BASE-SX, 1000BASE-LX, 100Base-TX (RJ45), 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 1000BASE-T
	5		Configurable Egress Queues	>= 8 per port including Strict Priority
	6		Power over Ethernet Options	- 802.3af (full power on all ports) - 802.3at (full power on all ports) - Configurable Power levels per port - Visibility into PoE power use
	7		Online Insertion/Removal Support	Required

High Density Modular LAN Access Switch				
ID	Ref. No.	Primary Attribute	Secondary Attribute	Specification
1	1	Chassis	Type	Modular
	2		19 Inch Rack Mounting	Required
	3		User Access Port Count	=> 144 copper or fiber
	4		System Throughput	Non-Blocking
	5		Packet Processor Redundancy	High Availability (critical areas): Required (Online Insertion/Removal) Non-Critical Areas: Not Required
	6		Packet Processor	Layer-3 Switching: Non-Blocking Layer-2 Switching: Non-Blocking
	7		Control Plane Redundancy Support	High Availability (critical areas): Required Non-Critical Areas: Not Required
	8		Cooling Redundancy Support	Required
	9		Power Supply Redundancy Support (1:1) or (N+1)	Required
	10		Input Power Options	AC
	11		Online Insertion/Removal Hot-Pluggable	Required
2	1	Operating System Features	Protocols switched in hardware	IPv4, IPv6, IGMP Snooping, IPv6 MLD v1 & v2
	2		Hot Swappable Insertion / Removal Support	Required
	3		Layer 3 Protocols & Routing Features	- IPv4, IPv6, ICMP, OSPF, BGP - Virtual Router Redundancy Protocol (VRRP) - Switching load sharing configurable per packet or per session, and per session is configuration with L3 address and L4 ports - Protocol Independent Multicast (PIM) v1 & v2
	4		OSPF Requirements	- IPv4 Open Shortest Path First (OSPF) versions 2 - IPv6 Open Shortest Path First (OSPF) versions 3 - MD5 authentication - Configurable areas, ABRs, and ASBRs - Configurable area types: normal (LSAs 1-5), stubby (LSAs 1-4), totally stubby (LSAs 1-2), Not-So-Stubby Area (NSSA) (LSAs 1-4 & 7), and NSSA totally stubby (LSAs 1-2 & 7) - Configurable router ID - Configurable hello packet interval - Configurable router dead interval - Configurable priority for DR and BDR - Configurable per interface network types (P2P, broadcast, NBMA, and virtual links) - Configurable cost per interface - Configurable cost multiplier - Ability to redistribute static routes and other protocol routes using access lists and route maps
	5		BGPv4 Requirements	- Multiprotocol Border Gateway Protocol (BGP) for IPv4 and IPv6 - MD5 authentication - Use all standard attributes - Ability to enable or disable synchronization - Configurable local preference per neighbor - Configurable multi-exit discriminator (MED) per neighbor - Configurable standard and extended communities

	6		Required L2 Features	802.1q, Per-port broadcast, multicast, and unicast storm control, 802.3ad (LACP), Link-Layer Discover Protocol, Jumbo Ethernet Frames with MTU up to 9000 bytes
	7		Port Security	- 802.1x Support - MAC Authentication Bypass - Dynamic VLAN Assignment - Configurable number of MAC Addresses allowed per port - Configurable actions to take when violation occurs - Ability to configure MAC address or addresses allowed per port - Ability to learn and stick a MAC Address per port
	8		QoS Features	- 802.1p class-of-service(CoS) classification - Differentiated Services Code Point (DSCP) classification - Support ingress classification, policing, and marking per port - Support egress queuing/scheduling
	9		Access Control Lists	- Access lists in hardware - Support for access lists source and destination L2 MAC address, Ethernet types, and SAPs - Support for access lists source and destination L3 addresses with masks and L4 port numbers - Support for prefix lists - Ability to apply L3 access list to L2 interfaces/ports - Ability to police (rate limit) per port, per port channel, per VLAN
	10		NTP Support	- Version 3 or greater Required - Configurable NTP Peer and Server Associations - Configurable NTP Authentication - Configurable NTP Access Restrictions - Configurable Source IP Address for NTP packets - Configurable Timezone/Offset - Configurable automatic recurring daylight savings time - Configurable per Interface
	11		Unidirectional Link Failure Detection	Required
	12		802.1d Required Spanning Tree Features	- Must be able to disable spanning tree per port - Ability to transition immediately to forwarding state per port on edge ports with 802.1d/s/w - Ability to disable topology change notifications per port on edge ports with 802.1d/s/w - STP cost configurable per port (0 to 240) 802.1d & 802.1t - STP priority configurable per VLAN (0 to 61,440) 802.1d & 802.1t - Ability to prevent rogue bridges from becoming the STP root - Ability to prevent an alternate port or a root port from assuming a designated port role due to the absence of BPDUs. - Ability to configure STP edge ports to disable upon receiving a BPDU

3	13		Network Management	- Centralized AAA w/ Role Based Authorization, Syslog, SNMP v2c, v3, SNMP Traps, SSH, Telnet, Radius or similar - Ability to disable telnet, ftp, http, https - IPv6 Support - Secure console port with roles based AAA authentication - Configurable Console & VTY timeout - Ability to define and apply IP access control lists to VTY sessions - Out of Band Ethernet Management Port -Optional - DNS support for resolution of user-defined device names
	14		SNMP Features	- Support for, SNMPv2C, & SNMPv3 - Support for traps that is an agent on the switch to send an unsolicited notifications to the SNMP manager for a configured event. - Configurable source IP address or interface for traps. - Supports both read-only (RO) and read-write (RW) community strings - Ability to restrict each community string to specific IP addresses independently - Ability to configure different SNMP versions for each SNMP manager -Support for multiple RO and RW community strings -Support for multiple SNMP profiles
	15		Port Mirroring or Similar	Required
	16		Remote Port Mirroring or Similar	Required
	17		Configuration File Management	TFTP, FTP
	18		Software Image Management	TFTP, FTP
	19		VLAN Support	>= 1000 VLAN's
	20		Data Traffic Rate Limiting	- Source and Destination IP - Layer 4 TCP and UDP - Source and Destination MAC
	21		VOIP Features	Configurable Voice-VLAN
	22		Message Logging Buffer	- Configurable log history size - Configurable logging severity - Configurable log message time stamps
	1		Throughput to Backplane	Non-Blocking option available
	2		Port per ASIC (Oversubscription)	1:1 Available option required
	3		Access Port Speed Options	- 10/100 Mbps Ethernet - 10/100/1000 Mbps Ethernet - 1 Gbps Ethernet (SFP)
	4		Uplink Port Speed Options	>= Qty 2 - 1 Gbps or 10 Gbps
3	5	Linecards / Port Interfaces	Media Flexibility Support	MMF >= 220m, SMF >= 10km, IEEE 802.3z-compliant 1000BASE-SX, 1000BASE-LX, 100Base-TX (RJ45), 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 1000BASE-T
	6		Configurable Egress Queues	>= 8 per port including Strict Priority
	7		Power over Ethernet Options	- 802.3af support (full power on all ports) - 802.3at support (full power on all ports) - Configurable Power levels per port - Visibility into PoE power use
	8		Online Insertion/Removal Support	Required

Stackable Network Access Switch				
ID	Ref. No.	Primary Attribute	Secondary Attribute	Specification
1	1	Chassis	Type	Fixed Configuration
	2		19 Inch Rack Mounting	Required
	3		Stacking Support for Multiple Switches	- Backplane (no user or uplink ports used to stack) - Single control-plane - Single data-plane - Non-Blocking optional
	4		Power Input Options	AC
	5		Redundant Power Option (1:1)	Optional High Availability Option: Required Non-Critical Option: Not Required
2	1	Packet Processor	Layer 2 Switching	Non-Blocking
	2		Layer 3 Switching	Non-Blocking
	3		IGMP Snooping & IPv6 MLD v1 & v2	Switched in Hardware
	4		MAC Addresses Per Switch	>=12000
3	1	Port Interfaces	Access Port Options	- 10/100 Mbps - 10/100/1000 Mbps - 1 Gbps Ethernet (SFP)
	2		Uplink Port Options	=> Qty 2 - 1 Gbps or 2 - 10 Gbps copper or fiber
	3		Per Switch Port Count Options	- 12 Port Option - 24 Port Option - 48 Port Option
	4		SFP Media Flexibility Options	IEEE 802.3z-compliant 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-T (RJ45), 100Base-T(RJ45), 10GBASE-SR, 10GBASE-LR
	5		Power over Ethernet Options	- 802.3af support (24 port & 48 port options, capable of supplying power to all ports) - 802.3at support (24 port & 48 port options) - Configurable power levels per port - Visibility into PoE power use
	6		Configurable Egress Queues	=> 8 per port including Strict Priority
4	1	Operating System	Layer 3 Protocols & Features	- IPv4, IPv6, ICMP, OSPF, BGP - Virtual Router Redundancy Protocol (VRRP) - Switching load sharing configurable per packet or per session, and per session is configuration with L3 address and L4 ports - Protocol Independent Multicast (PIM) v1 & v2

	2		OSPF Requirements	- IPv4 Open Shortest Path First (OSPF) versions 2 - IPv6 Open Shortest Path First (OSPF) versions 3 - MD5 authentication - Configurable areas, ABRs, and ASBRs - Configurable area types: normal (LSAs 1-5), stubby (LSAs 1-4), totally stubby (LSAs 1-2), Not-So-Stubby Area (NSSA) (LSAs 1-4 & 7), and NSSA totally stubby (LSAs 1-2 & 7) - Configurable router ID - Configurable hello packet interval - Configurable router dead interval - Configurable priority for DR and BDR - Configurable per interface network types (P2P, broadcast, NBMA, and virtual links) - Configurable cost per interface - Configurable cost multiplier - Ability to redistribute static routes and other protocol routes using access lists and route maps
	3		BGPv4 Requirements	- Multiprotocol Border Gateway Protocol (BGP) for IPv4 and IPv6 - MD5 authentication - Use all standard attributes - Ability to enable or disable synchronization - Configurable local preference per neighbor - Configurable multi-exit discriminator (MED) per neighbor - Configurable standard and extended communities
	4		Required L2 Features	802.1q, Per-port broadcast, multicast, and unicast storm control, 802.3ad (LACP), Link-Layer Discover Protocol, Jumbo Ethernet Frames with MTU up to 9000 bytes
	5		Port Security	- 802.1x Support - MAC Authentication Bypass - Dynamic VLAN Assignment - Configurable number of MAC Addresses allowed per port - Configurable actions to take when violation occurs - Ability to configure MAC address or addresses allowed per port - Ability to learn and stick a MAC Address per port
	6		QoS Features	- 802.1p class-of-service(CoS) classification - Differentiated Services Code Point (DSCP) classification - Support ingress classification, policing, and marking per port - Support egress queuing/scheduling

7		Access Control Lists	- Access lists in hardware - Support for access lists source and destination L2 MAC address, Ethernet types, and SAPs - Support for access lists source and destination L3 addresses with masks and L4 port numbers - Support for prefix lists - Ability to apply L3 access list to L2 interfaces/ports - Ability to police (rate limit) per port, per port channel, per VLAN
8		NTP Support	- Version 3 or greater Required - Configurable NTP Peer and Server Associations - Configurable NTP Authentication - Configurable NTP Access Restrictions - Configurable Source IP Address for NTP packets - Configurable Timezone/Offset - Configurable automatic recurring daylight savings time - Configurable per Interface
9		Unidirectional Link failure detection	Required
10		802.1d Required Spanning Tree Features	- Must be able to disable spanning tree per port - Ability to transition immediately to forwarding state per port on edge ports with 802.1d/s/w - Ability to disable topology change notifications per port on edge ports with 802.1d/s/w - STP cost configurable per port (0 to 240) 802.1d & 802.1t - STP priority configurable per VLAN (0 to 61,440) 802.1d & 802.1t - Ability to prevent rogue bridges from becoming the STP root - Ability to prevent an alternate port or a root port from assuming a designated port role due to the absence of BPDUs. - Ability to configure STP edge ports to disable upon receiving a BPDU
11		Network Management	- Centralized AAA w/ Role Based Authorization, Syslog, SNMP v2c, v3, SNMP Traps, SSH, Telnet, Radius or similar - Ability to disable telnet, ftp, http, https - IPv6 Support - Secure console port with roles based AAA authentication - Configurable Console & VTY timeout - Ability to define and apply IP access control lists to VTY sessions - Out of Band Ethernet Management Port -Optional - DNS support for resolution of user-defined device names
12		Multi-chassis Management Interface Aggregation	Required
13		Cross-Stack Link Aggregation	Required: must be capable to support defining link aggregation across multiple switches within a stack

14		SNMP Features	- Support for SNMPv2C, & SNMPv3 - Support for traps that is an agent on the switch to send an unsolicited notifications to the SNMP manager for a configured event. - Configurable source IP address or interface for traps. - Supports both read-only (RO) and read-write (RW) community strings - Ability to restrict each community string to specific IP addresses independently - Ability to configure different SNMP versions for each SNMP manager - Support for multiple RO and RW community strings - Support for multiple SNMP profiles
15		Port Mirroring or similar	Required
16		Remote Port Mirroring or similar	Required
17		Software Image Management	TFTP, FTP
18		Configuration File Management	TFTP, FTP
19		VLAN Support	>= 255 VLAN's >= 1000 VLAN ID's
20		Data Traffic Rate Limiting	- Source and Destination IP - Layer 4 TCP and UDP - Source and Destination MAC
21		VOIP Features	Configurable Voice-VLAN
22		Message Logging Buffer	- Configurable log history size - Configurable logging severity - Configurable log message time stamps

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

Modular LAN Campus Core Switch - Configuration				
ID	Ref. No.	Primary Attribute	Secondary Attribute	Specification
1	1	Chassis	Type	Modular
	2		19 Inch Rack Mounting	Required
	3		Redundant Switch Packet Processor	Required (Online Insertion/Removal)
	4		Packet Processor	Required
	5		Control Plane Redundancy Support	Required
	6		Cooling Redundancy Support	Required
	7		Power Supply Redundancy Support (1:1) or (N+1)	Required
	8		Input Power Options	AC Required
	9		Online Insertion/Removal Hot-Swappable	Required
	10		Multi-Chassis Link Aggregation Support	Required
2	1	Operating System Features	Protocols switched in hardware	IPv4, IPv6, IGMP Snooping, IPv6 MLD v1 & v2
	2		Layer 3 Protocols & Routing Features	- IPv4, IPv6, ICMP, OSPF, BGP - Virtual Router Redundancy Protocol (VRRP) - Routing Engine Fast failover - Switching load sharing configurable per packet or per session, and per session is configuration with L3 address and L4 ports - Protocol Independent Multicast (PIM) v1 & v2
	3		OSPF Requirements	- IPv4 Open Shortest Path First (OSPF) versions 2 - IPv6 Open Shortest Path First (OSPF) versions 3 - MD5 authentication - Configurable areas, ABRs, and ASBRs - Configurable area types: normal (LSAs 1-5), stubby (LSAs 1-4), totally stubby (LSAs 1-2), Not-So-Stubby Area (NSSA) (LSAs 1-4 & 7), and NSSA totally stubby (LSAs 1-2 & 7) - Configurable router ID - Configurable hello packet interval - Configurable router dead interval - Configurable priority for DR and BDR - Configurable per interface network types (P2P, broadcast, NBMA, and virtual links) - Configurable cost per interface - Configurable cost multiplier - Ability to redistribute static routes and other protocol routes using access lists and route maps
	4		BGPv4 Requirements	- Multiprotocol Border Gateway Protocol (BGP) for IPv4 and IPv6 - MD5 authentication - Use all standard attributes - Ability to enable or disable synchronization - Configurable local preference per neighbor - Configurable multi-exit discriminator (MED) per neighbor - Configurable standard and extended communities
	5		Required L2 Features	802.1q, Per-port broadcast, multicast, and unicast storm control, 802.3ad (LACP), Link-Layer Discover Protocol, Jumbo Ethernet Frames with MTU up to 9000 bytes

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

	6		Port Security Requirements	- 802.1x Support - MAC Authentication Bypass - Dynamic VLAN Assignment - Configurable number of MAC Addresses allowed per port - Configurable actions to take when violation occurs - Ability to configure MAC address or addresses allowed per port - Ability to learn and stick a MAC Address per port
	7		QoS Features	- 802.1p class-of-service(CoS) classification - Differentiated Services Code Point (DSCP) classification - Support ingress classification, policing, and marking per port - Support egress queuing/scheduling
	8		Access Control Lists	- Access lists in hardware - Support for access lists source and destination L2 MAC address, Ethernet types, and SAPs - Support for access lists source and destination L3 addresses with masks and L4 port numbers - Support for prefix lists - Ability to apply L3 access list to L2 interfaces/ports - Ability to police (rate limit) per port, per port channel, per VLAN
	9		NTP Support	- Version 3 or greater Required - Configurable NTP Peer and Server Associations - Configurable NTP Authentication - Configurable NTP Access Restrictions - Configurable Source IP Address for NTP packets - Configurable Timezone/Offset - Configurable automatic recurring daylight savings time - Configurable per Interface
	10		Unidirectional Link failure Detection	Required
	11		802.1d Required Spanning Tree Features	- Must be able to disable spanning tree per port - Ability to transition immediately to forwarding state per port on edge ports with 802.1d/s/w - Ability to disable topology change notifications per port on edge ports with 802.1d/s/w - STP cost configurable per port (0 to 240) 802.1d & 802.1t - STP priority configurable per VLAN (0 to 61,440) 802.1d & 802.1t - Ability to prevent rogue bridges from becoming the STP root - Ability to prevent an alternate port or a root port from assuming a designated port role due to the absence of BPDUs. - Ability to configure STP edge ports to disable upon receiving a BPDU

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

	12		Network Management	- Centralized AAA w/ Role Based Authorization, Syslog, SNMP v2c, v3, SNMP Traps, SSH, Telnet, Radius or similar - Ability to disable telnet, ftp, http, https - IPv6 Support - Secure console port with roles based AAA authentication - Configurable Console & VTY timeout - Ability to define and apply IP access control lists to VTY sessions - Out of Band Ethernet Management Port -Optional - DNS support for resolution of user-defined device names
	13		SNMP	- Support for, SNMPv2C, & SNMPv3 - Support for traps that is an agent on the switch to send an unsolicited notifications to the SNMP manager for a configured event. - Configurable source IP address or interface for traps. - Supports both read-only (RO) and read-write (RW) community strings - Ability to restrict each community string to specific IP addresses independently - Ability to configure different SNMP versions for each SNMP manager - Support for multiple RO and RW community strings - Support for multiple SNMP profiles
	14		Port Mirroring or similar	Required
	15		Remote Port Mirroring or similar	Required
	16		Configuration File Management	TFTP, FTP
	17		Software Image Management	TFTP, FTP
	3		Line-cards / Port Interfaces	Online Insertion/Removal Support
	1		Connection to Switch Fabric	=< 2:1 oversubscription
	2		Configurable Egress Queues	>= 8 per port including Strict Priority
	3		1 GbE Fiber port count	Minimum 144 count 1 GbE Fiber Ports (100 SX Optics) (44 LX/LH Optics)
	4		100/1000 port count	Minimum (48) 100/1000 Copper RJ45 ports
	5		10 GigE Port count	Minimum (2) 10 GigE Ports
	6			

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

High Density Modular LAN Access Switch - Configuration				
ID	Ref. No.	Primary Attribute	Secondary Attribute	Specification
1	1	Chassis	Type	Modular
	2		19 Inch Rack Mounting	Required
	3		System Throughput	Non-Blocking
	4		Packet Processor Redundancy	Required
	5		Packet Processor	Layer-3 Switching: Non-Blocking Layer-2 Switching: Non-Blocking
	6		Cooling Redundancy Support	Required
	7		Power Supply Redundancy Support (1:1) or (N+1)	Required
	8		Input Power Options	AC
	9		Online Insertion/Removal Hot-Pluggable Slot	Required
2	1	Operating System Features	Protocols switched in hardware	IPv4, IPv6, IGMP Snooping, IPv6 MLD v1 & v2
	2		Hot Swappable Insertion/Removal Support	Required
	3		Layer 3 Protocols & Routing Features	- IPv4, IPv6, ICMP, OSPF, BGP - Virtual Router Redundancy Protocol (VRRP) - Switching load sharing configurable per packet or per session, and per session is configuration with L3 address and L4 ports - Protocol Independent Multicast (PIM) v1 & v2
	4		QoS Features	- 802.1p class-of-service(CoS) classification - Differentiated Services Code Point (DSCP) classification - Support ingress classification, policing, and marking per port - Support egress queuing/scheduling
	5		Access Control Lists	- Access lists in hardware - Support for access lists source and destination L2 MAC address, Ethernet types, and SAPs - Support for access lists source and destination L3 addresses with masks and L4 port numbers - Support for prefix lists - Ability to apply L3 access list to L2 interfaces/ports - Ability to police (rate limit) per port, per port channel, per VLAN
	6		Port Security	- 802.1x Support - MAC Authentication Bypass - Dynamic VLAN Assignment - Configurable number of MAC Addresses allowed per port - Configurable actions to take when violation occurs - Ability to configure MAC address or addresses allowed per port - Ability to learn and stick a MAC Address per port
	7		Unidirectional Link failure Detection	Required

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

8		OSPF Requirements	- IPv4 Open Shortest Path First (OSPF) versions 2 - IPv6 Open Shortest Path First (OSPF) versions 3 - MD5 authentication - Configurable areas, ABRS, and ASBRs - Configurable area types: normal (LSAs 1-5), stubby (LSAs 1-4), totally stubby (LSAs 1-2), Not-So-Stubby Area (NSSA) (LSAs 1-4 & 7), and NSSA totally stubby (LSAs 1-2 & 7) - Configurable router ID - Configurable hello packet interval - Configurable router dead interval - Configurable priority for DR and BDR - Configurable per interface network types (P2P, broadcast, NBMA, and virtual links) - Configurable cost per interface - Configurable cost multiplier - Ability to redistribute static routes and other protocol routes using access lists and route maps
9		BGPv4 Requirements	- Multiprotocol Border Gateway Protocol (BGP) for IPv4 and IPv6 - MD5 authentication - Use all standard attributes - Ability to enable or disable synchronization - Configurable local preference per neighbor - Configurable multi-exit discriminator (MED) per neighbor - Configurable standard and extended communities
10		Required L2 Protocols & Features	- 802.1q - Per-port broadcast, multicast, and unicast storm control - 802.3ad (LACP) - Link-Layer Discover Protocol - Jumbo Ethernet Frames with MTU up to 9000 bytes
11		802.1d Spanning Tree Features Required	- Must be able to disable spanning tree per port - Ability to transition immediately to forwarding state per - port on edge ports with 802.1d/s/w - Ability to disable topology change notifications per port on edge ports with 802.1d/s/w - STP cost configurable per port (0 to 240) 802.1d & 802.1t - STP priority configurable per VLAN (0 to 61,440) 802.1d & 802.1t - Ability to prevent rogue bridges from becoming the STP root - Ability to prevent an alternate port or a root port from assuming a designated port role due to the absence of BPDUs. - Ability to configure STP edge ports to disable upon receiving a BPDU
12		VOIP Features	Configurable Voice-VLAN

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

	13		Network Management	- Centralized AAA w/ Role Based Authorization, Syslog, SNMP v2c, v3, SNMP Traps, SSH, Telnet, Radius or Similar - ability to disable telnet, ftp,HTTP, HTTPS - IPv6 Support - Secure console port with roles based AAA authentication - Configurable Console & VTY timeout - Ability to define and apply IP access control lists to VTY sessions - Out of Band Ethernet Management Port-optional - DNS support for resolution of user-defined device names		
	14		SNMP	- Support for SNMPv2C, & SNMPv3 - Support for traps that is an agent on the switch to send an unsolicited notifications to the SNMP manager for a configured event. - Configurable source IP address or interface for traps. - Supports both read-only (RO) and read-write (RW) community strings - Ability to restrict each community string to specific IP addresses independently - Ability to configure different SNMP versions for each SNMP manager - Support for multiple RO and RW community strings - Support for multiple SNMP profiles		
	15		Message Logging Buffer	- Configurable log history size - Configurable logging severity - Configurable log message time stamps		
	16		Port Mirroring or similar	Required		
	17		Remote Port Mirroring or similar	Required		
	18		Software Image Management	TFTP, FTP		
	19		Configuration file Backup and Management	TFTP, FTP		
	20		NTP Support	- Version 3 or greater Required - Configurable NTP Peer and Server Associations - Configurable NTP Authentication - Configurable NTP Access Restrictions - Configurable Source IP Address for NTP packets - Configurable Timezone/Offset - Configurable automatic recurring daylight savings time - Configurable per Interface		
	3		1	Linecards / Port Interfaces	Online Insertion/Removal	Required
	2		Connection to Switch Fabric		=< 2:1 oversubscription	
3	Configurable Egress Queues	>= 8 per port including Strict Priority				
4	Power over Ethernet Requirement	- 802.3af support (full power on all ports) - 802.3at support (full power on all ports) - Configurable Power levels per port - Visibility into PoE power use				
5	User Access Port Count	Minimum (240) ports of 100/1000 Copper RJ45				

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

	6		Uplink Ports Required	Minimum (4) 1 GbE Fiber (LX/LH Optics)
--	---	--	-----------------------	--

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

Stackable Network Access Switch - Configuration				
ID	Ref. No.	Primary Attribute	Secondary Attribute	Specification
1	1	Chassis	Type	Fixed Configuration
	2		19 Inch Rack Mounting	Required
	3		Stacking Support for Multiple Switches	- Backplane (no user or uplink ports used to stack) - Single control-plane - Single data-plane - Non-Blocking optional
	4			
	5		Power Supply Redundancy (1:1 or n+1)	Required
2	1	Packet Processor	Power Input Options	AC
	2		Layer 2 Switching Throughput (pps)	Non-Blocking
	3		Layer 3 Switching Throughput (pps)	Non-Blocking
3	1	Port Interfaces	IGMP Snooping & IPv6 MLD v1 & v2 in Hardware	Required
	2		User Access Port Count	(48) Port 100/1000 RJ45 Copper
	3		Uplink Ports	(4) GbE Fiber ports (LX/LH Optics)
	4		Power over Ethernet Options	- 802.3af support (all 48 ports) - 802.3at support (all 48 ports) - Configurable power levels per port - Visibility into PoE power use
	5			
4	1	Operating System	Configurable Egress Queues	=> 8 per port including Strict Priority
	2		Layer 3 Protocols & Features	- Option for L3 Switching: IPv4, IPv6, ICMP, OSPF, BGP - Virtual Router Redundancy Protocol (VRRP) - Switching load sharing configurable per packet or per session, and per session is configuration with L3 address and L4 ports - Protocol Independent Multicast (PIM) v1 & v2
			OSPF Requirements	- IPv4 Open Shortest Path First (OSPF) versions 2 - IPv6 Open Shortest Path First (OSPF) versions 3 - MD5 authentication - Configurable areas, ABRs, and ASBRs - Configurable area types: normal (LSAs 1-5), stubby (LSAs 1-4), totally stubby (LSAs 1-2), Not-So-Stubby Area (NSSA) (LSAs 1-4 & 7), and NSSA totally stubby (LSAs 1-2 & 7) - Configurable router ID - Configurable hello packet interval - Configurable router dead interval - Configurable priority for DR and BDR - Configurable per interface network types (P2P, broadcast, NBMA, and virtual links) - Configurable cost per interface - Configurable cost multiplier - Ability to redistribute static routes and other protocol routes using access lists and route maps

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

	3		BGPv4 Requirements	- Multiprotocol Border Gateway Protocol (BGP) for IPv4 and IPv6 - MD5 authentication - Use all standard attributes - Ability to enable or disable synchronization - Configurable local preference per neighbor - Configurable multi-exit discriminator (MED) per neighbor - Configurable standard and extended communities
	4		Layer 2 Protocols & Features	- 802.1q - Per-port broadcast, multicast, and unicast storm control - 802.3ad (LACP) - Link-Layer Discover Protocol - Jumbo Ethernet Frames with MTU up to 9000 bytes
	5		Port Security	- 802.1x Support - MAC Authentication Bypass - Dynamic VLAN Assignment - Configurable number of MAC Addresses allowed per port - Configurable actions to take when violation occurs - Ability to configure MAC address or addresses allowed per port - Ability to learn and stick a MAC Address per port
	6		Software Image Update Options	TFTP, FTP
	7		Configuration File Backup and Management	TFTP, FTP
	8		QoS Features	- 802.1p class-of-service(CoS) classification - Differentiated Services Code Point (DSCP) classification - Support ingress classification, policing, and marking per port - Support egress queuing/scheduling
	9		Access Control Lists	- Access lists in hardware - Support for access lists source and destination L2 MAC address, Ethernet types, and SAPs - Support for access lists source and destination L3 addresses with masks and L4 port numbers - Support for prefix lists - Ability to apply L3 access list to L2 interfaces/ports - Ability to police (rate limit) per port, per port channel, per VLAN
	10		NTP Support	- Version 3 or greater: Required - Configurable NTP Peer and Server Associations - Configurable NTP Authentication - Configurable NTP Access Restrictions - Configurable Source IP Address for NTP packets - Configurable Timezone/Offset - Configurable automatic recurring daylight savings time - Configurable per Interface
	11		Cross-Stack Link Aggregation	Required: must be capable to support defining link aggregation across multiple switches within a stack.

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

12		Unidirectional Link failure detection	Required
13		Port Mirroring or similar	Required
14		Remote Port Mirroring or similar	Required
15		Multi-chassis Management Interface Aggregation	Required
16		Network Management	- Centralized AAA w/ Role Based Authorization, Syslog, SNMP v2c, v3, SNMP Traps, SSH, Telnet, Radius or similar - Ability to disable telnet, ftp, http, https - IPv6 Support - Secure console port with roles based AAA authentication - Configurable Console & VTY timeout - Ability to define and apply IP access control lists to VTY sessions - Out of Band Ethernet Management port-optional - DNS support for resolution of user-defined device names
17		Message Logging Buffer	- Configurable log history size - Configurable logging severity - Configurable log message time stamps
18		Data Traffic Rate Limiting	- Source and Destination IP - Layer 4 TCP and UDP - Source and Destination MAC
19		VOIP Features	Configurable Voice-VLAN
20		SNMP	- Support for SNMPv2C, & SNMPv3 - Support for traps that is an agent on the switch to send an unsolicited notifications to the SNMP manager for a configured event. - Configurable source IP address or interface for traps. - Supports both read-only (RO) and read-write (RW) community strings - Ability to restrict each community string to specific IP addresses independently - Ability to configure different SNMP versions for each SNMP manager - Support for multiple RO and RW community strings - Support for multiple SNMP profiles
21		Required 802.1d Spanning Tree Features	- Must be able to disable spanning tree per port - Ability to transition immediately to forwarding state per port on edge ports with 802.1d/s/w - Ability to disable topology change notifications per port on edge ports with 802.1d/s/w - STP cost configurable per port (0 to 240) 802.1d & 802.1t - STP priority configurable per VLAN (0 to 61,440) 802.1d & 802.1t - Ability to prevent rogue bridges from becoming the STP root - Ability to prevent an alternate port or a root port from assuming a designated port role due to the absence of BPDUs. - Ability to configure STP edge ports to disable upon receiving a BPDU

Class A Router				
ID	Ref. No.	Primary Attribute	Secondary Attribute	Specification
1	1	Chassis	Type (Modular vs. Static)	Required: Modular
	2		Throughput	>= 15 Millions packets per second
	3		Packet Processor Redundancy	Required
	4		Control Plane Redundancy	Required
	5		Cooling Redundancy	Required: May be internal to power supplies
	6		Power Supply Redundancy	Required
	7		Front-Back Airflow	Required
	8		Online Insertion & Removal	Required
2	1	Packet Processor	Type (upgradable)	Required (Field Replaceable)
	2		Packet Processor Redundancy	Required
	3		Layer 3 Routing Throughput (PPS)	>= 15 Million packets per second
	4		Online Insertion & Removal	Required
	5		Memory (DRAM, Flash)	>= 2 GB – DRAM, 1 GB - Flash
3	1	Interface Cards	Interface Speed	Up to 10Gbps
	2		Interface Media Flexibility	Required (from T-1 to 10Gbps interfaces) T-1, channelized T-1, DS-3, channelized DS-3, OC-3 to OC12, OC-3 to OC-12 Packet over SONET, 10Mbps to 10Gbps Ethernet, at a minimum.
	3		Queuing Properties	Required: (see Operating System requirements)
	4		Online Insertion & Removal	Required
4	1	Operating System	Features Supported	Required: Routing, Bridging, Switching
	2		Routing Protocols	Required: BGPv4, OSPF
	3		OSPF Requirements	- IPv4 Open Shortest Path First (OSPF) versions 2 - IPv6 Open Shortest Path First (OSPF) versions 3 - MD5 authentication - Configurable areas, ABRs, and ASBRs - Configurable area types: normal (LSAs 1-5), stubby (LSAs 1-4), totally stubby (LSAs 1-2), Not-So-Stubby Area (NSSA) (LSAs 1-4 & 7), and NSSA totally stubby (LSAs 1-2 & 7) - Configurable router ID - Configurable hello packet interval - Configurable router dead interval - Configurable priority for DR and BDR - Configurable per interface network types (P2P, broadcast, NBMA, and virtual links) - Configurable cost per interface - Configurable cost multiplier - Ability to redistribute static routes and other protocol routes using access lists and route maps
	4		BGPv4 Requirements	- Multiprotocol Border Gateway Protocol (BGP) for IPv4 and IPv6 - MD5 authentication - Use all standard attributes - Ability to enable or disable synchronization - Configurable local preference per neighbor - Configurable multi-exit discriminator (MED) per neighbor - Configurable standard and extended communities
	5		Quality of Service	- Required: >=8 Queues including Strict Priority Queue - Shaping and policing - DSCP & IP Precedence

	6		Protocols Supported	Required: MPLS, IPv4, IPv6, 802.1Q, GRE, IPSEC, GDOI, PIM v1 & v2
	7		Access Control Lists	- Access lists in hardware - Support for access lists source and destination L2 MAC address, Ethernet types, and SAPs - Support for access lists source and destination L3 addresses with masks and L4 port numbers - Support for prefix lists - Ability to apply L3 access list to L2 interfaces/ports - Ability to police (rate limit) per port, per port channel, per VLAN
	8		SNMP Requirements	- Support for SNMPv2C, & SNMPv3 - Support for traps that is an agent on the switch to send an unsolicited notifications to the SNMP manager for a configured event. - Configurable source IP address or interface for traps. - Supports both read-only (RO) and read-write (RW) community strings - Ability to restrict each community string to specific IP addresses independently - Ability to configure different SNMP versions for each SNMP manager - Support for multiple RO and RW community strings - Support for multiple SNMP profiles
	9		Network Management	Required: Technology to monitor continuous traffic on the network, SNMPv2c and v3, SSH, SSL, Syslog, SNMP Traps, Centralized AAA, Netflow Version 9
5	1	WAN Encryption	FIPS 140-2 Certification	Required: Complete, or in process. (The system must be either FIPS 140-2 NIST certified or at least in stage 3 testing.)
	2		Throughput	Required: >= 5Gbps
	3		Hardware vs Software	Required: Hardware
	4		Latency	Required: <=100usec
	5		Protocols	Required: GDOI
	6		Supported Connection Count	Required: >=2000 encrypted tunnels
	7		Interface Type	Required: Encryption Supported on all interface types

Class B Router				
ID	Ref. No.	Primary Attribute	Secondary Attribute	Specification
1	1	Chassis	Type (Modular vs. Static)	Required: Modular
	2		Throughput	>= 2 Millions packets per second
	3		Packet Processor Redundancy	Required
	4		Control Plane Redundancy	Required
	5		Cooling Redundancy	Required
	6		Power Supply Redundancy	Required
	7		Front-Back Airflow	Not Required
	8		Online Insertion & Removal	Required
2	1	Packet Processor	Type (upgradable)	Required
	2		Packet Processor Redundancy	Required
	3		Layer 3 Routing Throughput (PPS)	>= 2 Million packets per second
	4		Online Insertion & Removal	Required
	5		Memory (DRAM, Flash)	>= 1 GB – DRAM, 256MB - Flash
3	1	Interface Cards	Interface Speed	Up to multiple OC-3
	2		Interface Media Flexibility	Required (from T-1 to OC-3 interfaces) T-1, channelized T-1, DS-3, channelized DS-3, OC-3, OC-3 Packet over SONET, 10 Mbps to 1 Gbps Ethernet, at a minimum.
	3		Queuing Properties	Required: (see Operating System requirements)
	4		Online Insertion & Removal	Required
4	1	Operating System	Features Supported	Required: Routing, Bridging, Switching
	2		Routing Protocols	Required: BGPv4, OSPF
	3		OSPF Requirements	- IPv4 Open Shortest Path First (OSPF) versions 2 - IPv6 Open Shortest Path First (OSPF) versions 3 - MD5 authentication - Configurable areas, ABRs, and ASBRs - Configurable area types: normal (LSAs 1-5), stubby (LSAs 1-4), totally stubby (LSAs 1-2), Not-So-Stubby Area (NSSA) (LSAs 1-4 & 7), and NSSA totally stubby (LSAs 1-2 & 7) - Configurable router ID - Configurable hello packet interval - Configurable router dead interval - Configurable priority for DR and BDR - Configurable per interface network types (P2P, broadcast, NBMA, and virtual links) - Configurable cost per interface - Configurable cost multiplier - Ability to redistribute static routes and other protocol routes using access lists and route maps
	4		BGPv4 Requirements	- Multiprotocol Border Gateway Protocol (BGP) for IPv4 and IPv6 - MD5 authentication - Use all standard attributes - Ability to enable or disable synchronization - Configurable local preference per neighbor - Configurable multi-exit discriminator (MED) per neighbor - Configurable standard and extended communities
	5		Quality of Service	- Required: >=8 Queues including Strict Priority Queue - Shaping and policing - DSCP & IP Precedence
	6		Protocols Supported	Required: MPLS, IPv4, IPv6, 802.1Q, GRE, IPSEC, GDOI, PIM v1 & v2

	7		Access Control Lists	- Access lists in hardware - Support for access lists source and destination L2 MAC address, Ethernet types, and SAPs - Support for access lists source and destination L3 addresses with masks and L4 port numbers - Support for prefix lists - Ability to apply L3 access list to L2 interfaces/ports - Ability to police (rate limit) per port, per port channel, per VLAN
	8		SNMP Requirements	- Support for SNMPv2C, & SNMPv3 - Support for traps that is an agent on the switch to send an unsolicited notifications to the SNMP manager for a configured event. - Configurable source IP address or interface for traps. - Supports both read-only (RO) and read-write (RW) community strings - Ability to restrict each community string to specific IP addresses independently - Ability to configure different SNMP versions for each SNMP manager -Support for multiple RO and RW community strings -Support for multiple SNMP profiles
	9		Network Management	Required: Technology to monitor continuous traffic on the network, SNMPv2c and v3, SSH, SSL, Syslog, SNMP Traps, Centralized AAA, Netflow Version 9
5	1	WAN Encryption	FIPS 140-2 Certification	Required: Complete, or in process. (The system must be either FIPS 140-2 NIST certified or at least in stage 3 testing.)
	2		Throughput	Required: >= 900Mbps
	3		Hardware vs Software	Required: Hardware
	4		Latency	Required: <=100usec
	5		Protocols	Required: GDOI
	6		Supported Connection Count	Required: >=2000 encrypted tunnels
	7		Interface Type	Required: Encryption Supported on all interface types

Class C Router					
ID	Ref. No.	Primary Attribute	Secondary Attribute	Specification	
1	1	Chassis	Type	Fixed or Modular	
	2		Throughput	>= 500k packets per second	
	3		Packet Processor Redundancy	Not Required	
	4		Control Plane Redundancy	Not Required	
	5		Cooling Redundancy	Not Required	
	6		Power Supply Redundancy	Not Required	
	7		Front-Back Airflow	Not Required	
	8		Online Insertion & Removal	Not Required	
2	1	Packet Processor	Type (upgradable)	Not Required	
	2		Layer 3 Routing Throughput (PPS)	>= 500k packets per second	
	3		Online Insertion & Removal	Not Required	
	4		Memory (DRAM, Flash)	>= 1 GB – DRAM, 256MB - Flash	
3	1	Interface Cards	Interface Speed	Up to multiple DS3	
	2		Interface Media Flexibility	Required (from T-1 to DS3 interfaces) T-1, channelized T-1, DS-3, channelized DS-3, 10 Mbps to 1 Gbps Ethernet, at a minimum.	
	3			Queuing Properties	Required: => 8 queues including a Strict Priority Queue (see Operating System requirements)
	4		Online Insertion & Removal	Not Required	
4	1	Operating System	Features Supported	Required: Routing, Bridging, Switching	
	2		Routing Protocols	Required: BGPv4, OSPF	
	3		OSPF Requirements	- IPv4 Open Shortest Path First (OSPF) versions 2 - IPv6 Open Shortest Path First (OSPF) versions 3 - MD5 authentication - Configurable areas, ABRS, and ASBRs - Configurable area types: normal (LSAs 1-5), stubby (LSAs 1-4), totally stubby (LSAs 1-2), Not-So-Stubby Area (NSSA) (LSAs 1-4 & 7), and NSSA totally stubby (LSAs 1-2 & 7) - Configurable router ID - Configurable hello packet interval - Configurable router dead interval - Configurable priority for DR and BDR - Configurable per interface network types (P2P, broadcast, NBMA, and virtual links) - Configurable cost per interface - Configurable cost multiplier - Ability to redistribute static routes and other protocol routes using access lists and route maps	
	4			BGPv4 Requirements	- Multiprotocol Border Gateway Protocol (BGP) for IPv4 and IPv6 -MD5 authentication -use all standard attributes -ability to enable or disable synchronization -Configurable local preference per neighbor -Configurable multi-exit discriminator (MED) per neighbor -Configurable standard and extended communities
	5				Quality of Service
	6		Protocols Supported	Required: MPLS, IPv4, IPv6, 802.1Q, GRE, IPSEC, GDOI, PIM v1 & v2	

	7		Access Control Lists	-Access lists in hardware -support for access lists source and destination L2 MAC address, Ethernet types, and SAPs - Support for access lists source and destination L3 addresses with masks and L4 port numbers - Support for prefix lists - Ability to apply L3 access list to L2 interfaces/ports - Ability to police (rate limit) per port, per port channel, per VLAN
	8		SNMP Requirements	- Support for SNMPv2C, & SNMPv3 - Support for traps that is an agent on the switch to send an unsolicited notifications to the SNMP manager for a configured event. - Configurable source IP address or interface for traps. - Supports both read-only (RO) and read-write (RW) community strings - Ability to restrict each community string to specific IP addresses independently - Ability to configure different SNMP versions for each SNMP manager - Support for multiple RO and RW community strings - Support for multiple SNMP profiles
	9		Network Management	Required: Technology to monitor continuous traffic on the network, SNMPv2c and v3, SSH, SSL, Syslog, SNMP Traps, Centralized AAA, Netflow Version 9
5	1	WAN Encryption	FIPS 140-2 Certification	Required: Complete, or in process. (The system must be either FIPS 140-2 NIST certified or at least in stage 3 testing.)
	2		Throughput	Required: >= 200Mbps
	3		Hardware vs Software	Required: Hardware
	4		Latency	Required: <=100usec
	5		Protocols	Required: GDOI
	6		Supported Connection Count	Required: >=1000 encrypted tunnels
	7		Interface Type	Required: Encryption Supported on all interface types

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

Class A Router - Configuration				
ID	Ref. No.	Primary Attribute	Secondary Attribute	Specification
1	1	Chassis	Type	Required: Modular
	2		Throughput	>= 15 Millions packets per second
	3		Packet Processor Redundancy	Required
	4		Control Plane Redundancy	Required
	5		Cooling Redundancy	Required
	6		Power Supply Redundancy	Required
	7		Front-Back Airflow	Required
	8		Online Insertion & Removal	Required
2	1	Packet Processor	Type (upgradable)	Required (Field Replaceable)
	2		Packet Processor Redundancy	Required
	3		Layer 3 Routing Throughput (PPS)	Non-Blocking
	4		Memory (DRAM, Flash)	Include maximum DRAM and Flash available
	5		Online Insertion & Removal	Required
3	1	Interface Cards	WAN Interfaces	Qty (2) 1 GbE (SX Optics) - individually Field Replaceable
	2		LAN Interfaces	Qty (2) 1 GbE fiber ports (SX Optics) - individually Field Replaceable
	3		Egress Queuing Properties	Required: => 8 queues including a Strict Priority Queue
	4		Online Insertion & Removal	Required
4	1	Operating System	Features Supported	Required: Routing, Bridging, Switching
	2		Routing Protocols	Required: BGPv4, OSPF
	3		OSPF Requirements	- IPv4 Open Shortest Path First (OSPF) versions 2 - IPv6 Open Shortest Path First (OSPF) versions 3 - MD5 authentication - Configurable areas, ABRS, and ASBRs - Configurable area types: normal (LSAs 1-5), stubby (LSAs 1-4), totally stubby (LSAs 1-2), Not-So-Stubby Area (NSSA) (LSAs 1-4 & 7), and NSSA totally stubby (LSAs 1-2 & 7) - Configurable router ID - Configurable hello packet interval - Configurable router dead interval - Configurable priority for DR and BDR - Configurable per interface network types (P2P, broadcast, NBMA, and virtual links) - Configurable cost per interface - Configurable cost multiplier - Ability to redistribute static routes and other protocol routes using access lists and route maps
	4		BGPv4 Requirements	- Multiprotocol Border Gateway Protocol (BGP) for IPv4 and IPv6 - MD5 authentication - Use all standard attributes - Ability to enable or disable synchronization - Configurable local preference per neighbor - Configurable multi-exit discriminator (MED) per neighbor - Configurable standard and extended communities
	5		Quality of Service	Required: >=8 Queues including Strict Priority Queue - Shaping and policing - DSCP & IP Precedence

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

	6		Protocols Supported	Required: MPLS, IPv4, IPv6, 802.1Q, GRE, IPSEC, GDOI, PIM v1 & v2
	7		Network Management	Required: Technology to monitor continuous traffic on the network, SNMPv2c and v3, SSH, SSL, Syslog, SNMP Traps, Centralized AAA, Netflow Version 9
	8		SNMP Requirements	- Support for SNMPv2C, & SNMPv3 - Support for traps that is an agent on the switch to send an unsolicited notifications to the SNMP manager for a configured event. - Configurable source IP address or interface for traps. - Supports both read-only (RO) and read-write (RW) community strings - Ability to restrict each community string to specific IP addresses independently - Ability to configure different SNMP versions for each SNMP manager - Support for multiple RO and RW community strings - Support for multiple SNMP profiles
	9		Access Control Lists	- Access lists in hardware - Support for access lists source and destination L2 MAC address, Ethernet types, and SAPs - Support for access lists source and destination L3 addresses with masks and L4 port numbers - Support for prefix lists - Ability to apply L3 access list to L2 interfaces/ports - Ability to police (rate limit) per port, per port channel, per VLAN
5	1	WAN Encryption	FIPS 140-2 Certification	Required: Complete, or in process. (The system must be either FIPS 140-2 NIST certified or at least in stage 3 testing.)
	2		Throughput	Required: >= 5Gbps
	3		Hardware vs Software	Required: Hardware
	4		Latency	Required: <=100usec
	5		Protocols	Required: GDOI
	6		Supported Connection Count	Required: >=2000 encrypted tunnels
	7		Interface Type	Required: Encryption Supported on all interface types

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

Class B Router - Configuration				
ID	Ref. No.	Primary Attribute	Secondary Attribute	Specification
1	1	Chassis	Type	Required: Modular
	2		Throughput	>= 2 Millions packets per second
	3		Packet Processor Redundancy	Required
	4		Control Plane Redundancy	Required
	5		Cooling Redundancy	Required
	6		Power Supply Redundancy	Required
	7		Online Insertion & Removal	Required
2	1	Packet Processor	Type (upgradable)	Required
	2		Packet Processor Redundancy	Required
	3		Layer 3 Routing Throughput (PPS)	>= 2 Million packets per second
	4		Memory (DRAM, Flash)	Include maximum DRAM and Flash available
	5		Online Insertion & Removal	Required
3	1	Interface Cards	WAN Interface	Qty (2) OC3 POS (Short Range multimode optics)
	2		LAN Interfaces	Qty (2) 1 GbE fiber ports (SX Optics) - individually Field Replaceable
	3		Egress Queuing Properties	Required: => 8 queues including a Strict Priority Queue
	4		Online Insertion & Removal	Required
4	1	Operating System	Features Supported	Required: Routing, Bridging, Switching
	2		Routing Protocols	Required: BGPv4, OSPF
	3		OSPF Requirements	- IPv4 Open Shortest Path First (OSPF) versions 2 - IPv6 Open Shortest Path First (OSPF) versions 3 - MD5 authentication - Configurable areas, ABRS, and ASBRs - Configurable area types: normal (LSAs 1-5), stubby (LSAs 1-4), totally stubby (LSAs 1-2), Not-So-Stubby Area (NSSA) (LSAs 1-4 & 7), and NSSA totally stubby (LSAs 1-2 & 7) - Configurable router ID - Configurable hello packet interval - Configurable router dead interval - Configurable priority for DR and BDR - Configurable per interface network types (P2P, broadcast, NBMA, and virtual links) - Configurable cost per interface - Configurable cost multiplier - Ability to redistribute static routes and other protocol routes using access lists and route maps
	4		BGPv4 Requirements	- Multiprotocol Border Gateway Protocol (BGP) for IPv4 and IPv6 - MD5 authentication - Use all standard attributes - Ability to enable or disable synchronization - Configurable local preference per neighbor - Configurable multi-exit discriminator (MED) per neighbor - Configurable standard and extended communities
	5		Quality of Service	Required: >=8 Egress Queues including Strict Priority Queue - Shaping and policing - DSCP & IP Precedence
	6		Protocols Supported	Required: MPLS, IPv4, IPv6, 802.1Q, GRE, IPSEC, GDOI, PIM v1 & v2

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

	7		Access Control Lists	- Access lists in hardware - Support for access lists source and destination L2 MAC address, Ethernet types, and SAPs - Support for access lists source and destination L3 addresses with masks and L4 port numbers - Support for prefix lists - Ability to apply L3 access list to L2 interfaces/ports - Ability to police (rate limit) per port, per port channel, per VLAN
	8		Network Management	Required: Technology to monitor continuous traffic on the network, SNMPv2c and v3, SSH, SSL, Syslog, SNMP Traps, Centralized AAA, Netflow Version 9
	9		SNMP Requirements	- Support for SNMPv2C, & SNMPv3 - Support for traps that is an agent on the switch to send an unsolicited notifications to the SNMP manager for a configured event. - Configurable source IP address or interface for traps. - Supports both read-only (RO) and read-write (RW) community strings - Ability to restrict each community string to specific IP addresses independently - Ability to configure different SNMP versions for each SNMP manager - Support for multiple RO and RW community strings - Support for multiple SNMP profiles
5	1	WAN Encryption	FIPS 140-2 Certification	Required: Complete, or in process. (The system must be either FIPS 140-2 NIST certified or at least in stage 3 testing.)
	2		Throughput	Required: >= 900Mbps
	3		Hardware vs Software	Required: Hardware
	4		Latency	Required: <=100usec
	5		Protocols	Required: GDOI
	6		Supported Connection Count	Required: >=2000 encrypted tunnels
	7		Interface Type	Required: Encryption Supported on all interface types

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

Class C Router - Configuration				
ID	Ref. No.	Primary Attribute	Secondary Attribute	Specification
1	1	Chassis	Type	Fixed or Modular
	2		Throughput	>= 500k packets per second
	3		Packet Processor Redundancy	Not Required
	4		Control Plane Redundancy	Not Required
	5		Cooling Redundancy	Not Required
	6		Power Supply Redundancy	Not Required
	7		Online Insertion & Removal	Not Required
2	1	Packet Processor	Layer 3 Routing Throughput (PPS)	>= 500k packets per second
	2		Memory (DRAM, Flash)	Include maximum DRAM and Flash available
3	1	Interface Cards	WAN Interface	Qty (2) DS3
	2		LAN Interfaces	Qty (1) 1 GbE ports (SFP – Copper RJ45)
	3		Egress Queuing Properties	Required: => 8 queues including a Strict Priority Queue
	4		Online Insertion & Removal	Not Required
4	1	Operating System	Features Supported	Required: Routing, Bridging, Switching
	2		Routing Protocols	Required: BGPv4, OSPF
	3		OSPF Requirements	- IPv4 Open Shortest Path First (OSPF) versions 2 - IPv6 Open Shortest Path First (OSPF) versions 3 - MD5 authentication - Configurable areas, ABRS, and ASBRs - Configurable area types: normal (LSAs 1-5), stubby (LSAs 1-4), totally stubby (LSAs 1-2), Not-So-Stubby Area (NSSA) (LSAs 1-4 & 7), and NSSA totally stubby (LSAs 1-2 & 7) - Configurable router ID - Configurable hello packet interval - Configurable router dead interval - Configurable priority for DR and BDR - Configurable per interface network types (P2P, broadcast, NBMA, and virtual links) - Configurable cost per interface - Configurable cost multiplier - Ability to redistribute static routes and other protocol routes using access lists and route maps
	4		BGPv4 Requirements	- Multiprotocol Border Gateway Protocol (BGP) for IPv4 and IPv6 - MD5 authentication - Use all standard attributes - Ability to enable or disable synchronization - Configurable local preference per neighbor - Configurable multi-exit discriminator (MED) per neighbor - Configurable standard and extended communities
	5		Quality of Service	Required: >=8 Queues including Strict Priority Queue - Shaping and policing - DSCP & IP Precedence
	6		Protocols Supported	Required: MPLS, IPv4, IPv6, 802.1Q, GRE, IPSEC, GDOI, PIM v1 & v2

Configuration Item Addendum

Note: This addendum represents one of the most complex variants and has been created for pricing purposes only.

	7		Access Control Lists	- Access lists in hardware - Support for access lists source and destination L2 MAC address, Ethernet types, and SAPs - Support for access lists source and destination L3 addresses with masks and L4 port numbers - Support for prefix lists - Ability to apply L3 access list to L2 interfaces/ports - Ability to police (rate limit) per port, per port channel, per VLAN
	8		SNMP Requirements	- Support for SNMPv2C, & SNMPv3 - Support for traps that is an agent on the switch to send an unsolicited notifications to the SNMP manager for a configured event. - Configurable source IP address or interface for traps. - Supports both read-only (RO) and read-write (RW) community strings - Ability to restrict each community string to specific IP addresses independently - Ability to configure different SNMP versions for each SNMP manager - Support for multiple RO and RW community strings - Support for multiple SNMP profiles
	9		Network Management	Required: Technology to monitor continuous traffic on the network, SNMPv2c and v3, SSH, SSL, Syslog, SNMP Traps, Centralized AAA, Netflow Version 9
5	1	WAN Encryption	FIPS 140-2 Certification	Required: Complete, or in process. (The system must be either FIPS 140-2 NIST certified or at least in stage 3 testing.)
	2		Throughput	Required: >= 200 Mbps
	3		Hardware vs Software	Required: Hardware
	4		Latency	Required: <=100usec
	5		Protocols	Required: GDOI
	6		Supported Connection Count	Required: >=1000 encrypted tunnels
	7		Interface Type	Required: Encryption Supported on all interface types

	Fiber Channel DAS Storage
	OEM & Model/Part Number:
Reference Number	Requirements (Note: JBOD Configuration with Basic Level Raid Functionality.)
1	Solution Shall Meet a minimum of the following IOPS (I/Os per second) 180 per drive.
2	Solution Shall Meet a minimum of the following throughput (Mbits per second) 400 per drive.
3	Solution Shall Meet the following minimum usable total disk space: 1 TB.
4	Shall Provide dual ported drives with connections to drive enclosure(s).
5	Solution Shall Provide the capability of supporting a JBOD configuration of the following Drive Type (Protocol/Interface): Fibre Channel.
6	Overall Solution Shall Provide a multiple physical drive count that will meet requirements for IOPS, throughput and capacity (specified at Delivery Order Level).
7	Solution Shall Provide the ability to allow non-disruptive updates or upgrades to drive firmware when used with an External Raid controller that supports this function.
8	Solution Shall Provide ability to configure disk drives by an External Raid controller and meet IOPs, Throughput and Capacity requirements above.

	SAS DAS Storage
	OEM Model/Part Number:
Reference Number	Requirements (Note: JBOD Configuration with Basic Level Raid Functionality.)
1	Solution Shall Meet a minimum of the following IOPS (I/Os per second) 180 per drive (15K) and 130 per drive (10K).
2	Solution Shall Meet a minimum of the following throughput (Mbits per second) 300 per drive.
3	Solution Shall Meet the following minimum usable total disk space: 2 TB.
4	Shall Provide dual ported drives with connections to drive enclosure(s).
5	Solution Shall Provide drive(s) that support data transfer speeds up to 6 Gbit/s.
6	Solution Shall Provide the capability of supporting a JBOD configuration of the following Drive Type (Protocol/Interface): SAS
7	Overall Solution Shall Provide a multiple physical drive count that will meet requirements for IOPS, throughput and capacity (specified at Delivery Order Level).
8	Solution Shall Provide the ability to allow non-disruptive updates or upgrades to drive firmware when used with an External Raid controller that supports this function.
9	Solution Shall Provide ability to configure disk drives by an External Raid controller and meet IOPS, Throughput and Capacity requirements above.

	SATA DAS Storage
	OEM Model/Part Number:
Reference Number	Requirements (Note: JBOD Configuration with Basic Level Raid Functionality.)
1	Solution Shall Meet a minimum of following IOPS (I/Os per second) 80 per drive at 7200 RPM.
2	Solution Shall Meet a minimum of the following throughput (Mbits per second) 200 per drive.
3	Solution Shall Meet the following minimum usable total disk space: 2 TB.
4	Solution Shall Provide drive(s) that support data transfer speeds up to 6 Gbit/s.
5	Solution Shall Provide the capability of supporting a JBOD configuration of the following Drive Type (Protocol/Interface): Enterprise Level SATA (Nearline SAS or NL-SAS interface).
6	Overall Solution Shall Provide a multiple physical drive count that will meet requirements for IOPS, throughput and capacity (specified at Delivery Order Level).
7	Solution Shall Provide the ability to allow non-disruptive updates or upgrades to drive firmware when used with an External Raid controller that supports this function.
8	Solution Shall Provide ability to configure disk drives by an External Raid controller and meet IOPS, Throughput and Capacity requirements above.

	SSD DAS Storage
	OEM Model/Part Number:
Reference Number	Requirements (Note: JBOD Configuration with Basic Level Raid Functionality.)
1	Solution Shall Meet a minimum of the following IOPS (I/Os per second) 4000 per Drive.
2	Solution Shall Meet a minimum of the following throughput (Mbits per second): write=250/read=350. Vendor shall provide Performance numbers using 4K blocks, doing both Sequential and Random Reads and Writes.
3	Solution Shall Provide the following, an equally balanced throughput for read and writes operations of a minimum of 250 Mb/s. Vendor shall provide Performance numbers using 4K blocks, doing both, Sequential and Random Reads and Writes.
4	Solution Shall Provide the following minimum usable total disk space: 400 GB.
5	Solution Shall Provide support for the following type of drive in a JBOD configuration: SSD.
6	Solution Shall Provide the capability of supporting one of the following Drive Types in a JBOD configuration with parallel NAND flash chips: SSD (Flash-Memory eMLC (enterprise Multi-Level Cell) or SLC (Single Level Cell) DRAM or RAM based).
7	Flash-Memory eMLC (enterprise Multi-Level Cell) will support minimum of 8,000 erase/write operations.
8	Flash-Memory SLC (Single-Level Cell) will support minimum of 80,000 erase/write operations.
9	Overall Solution Shall Provide a multiple physical drive count that will meet requirements for IOPS, throughput and capacity (specified at Delivery Order Level).
10	Solution Shall Provide the ability to allow non-disruptive updates or upgrades to drive firmware when used with an External Raid controller that supports this function.
11	Solution Shall Provide ability to configure disk drives by an External Raid controller and meet IOPs, Throughput and Capacity requirements above.

Low Performance SAN Storage	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support a minimum of 20,000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
2	Shall support minimum aggregate data rate of 2000 MBytes per second for all read or write or combination of read/write operations through the storage subsystem.
3	Shall provide the minimum usable native disk capacity of 25 TB without compression or deduplication.
4	Shall be capable of supporting a minimum of two (2) 8-Gbit/s Fibre Channel ports per controller. All Fibre Channel ports shall be capable of autosensing slower speeds of 2 and 4 Gbit/s.
5	Shall be capable of supporting a minimum of two (2) 1GbE iSCSI ports per controller.
6	Shall be capable of supporting a minimum of one (1) 10GbE iSCSI ports per controller.
7	Shall be capable of supporting Jumbo frame and LACP protocol.
8	Minimum shall be capable of supporting Fibre Channel (FC) or Internet Small Computer System Interface (iSCSI) connectivity on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
9	Shall provide the ability to expand iSCSI ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
10	Shall be capable of supporting native 10GbE host connections.
11	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
12	Solution shall support a minimum of 256 iSCSI initiators (host connections).

13	Minimum shall be capable of supporting Fibre Channel (FC) connectivity on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
14	Shall provide, excluding space on Storage System Operating System (OS) Drives, the initial data storage capacity must be distributed evenly among multiple shelves and support mirroring between shelves.
15	Shall provide the disk failure redundancy configuration to meet the capacity, IOPs and workload performance requirements (to be specified at delivery order level).
16	Shall provide the disk drive technologies to meet the capacity, IOPs and workload performance requirements (to be specified at delivery order level).
17	Shall provide capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
18	Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.
19	Shall provide a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
20	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
21	Shall provide a minimum of two storage controllers in a module for controller based storage solution, which are load balanced and provide automatic failover including the ability to maintain access to all data through a controller failure.
22	Shall provide the ability to upgrade a controller on the storage system without replacing the storage subsystem and the upgrade of the controller shall be non-destructive to the data, requiring no data migration, no reconfiguration and no LUN remapping to any connecting Host.

23	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
24	Shall provide the ability to expand and scale Host side connectivity and backend capacity, independently in order to increase performance.
25	Shall provide storage subsystem support boot from SAN.
26	Shall support the ability to manually change LUN UDID value.
27	Shall support the ability to create LUNs and volumes across multiple spindles.
28	Shall support non-disruptive LUN and volume expansion.
29	Shall support ability to present a minimum of a 15TB LUN/volume to a host.
30	Shall provide the ability to use "Thin Provisioning" or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
31	Shall provide that storage subsystem performance will not be affected when using "Thin Provisioning".
32	Shall provide the ability to expand Fibre Channel ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
33	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
34	Shall provide the capability of synchronous and asynchronous replication with write order fidelity.
35	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
36	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
37	Shall be capable of maintaining redundancy and the performance metrics requirements as stated above during snapshot and clone operations.
38	Power Switches shall be covered to prevent inadvertent activation.

39	Shall provide role-based security or audit trail logging for access to storage.
40	Shall provide a single master management interface to manage multiple storage subsystem of the same type in data center implementations.
41	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
42	Shall have a graphical user interface (GUI) or command (CLI), or a Wizard to automate the process to provision a large number of Disk Groups and LUNs.
43	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.
44	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.
45	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

Medium Performance SAN Storage	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support a minimum of 50,000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
2	Shall support minimum aggregate data rate of 3500 MBytes per second for all read or write or combination of read/write operations through the storage subsystem.
3	Shall provide the minimum usable native disk capacity of 50 TB without compression or deduplication.
4	Shall be capable of supporting a minimum of four (4) 8-Gbit/s Fibre Channel ports per controller. All Fibre Channel ports shall be capable of autosensing slower speeds of 2 and 4 Gbit/s.
5	Shall be capable of supporting a minimum of four (4) 1GbE iSCSI ports per controller.
6	Shall be capable of supporting a minimum of two (2) 10GbE iSCSI ports per controller.
7	Shall be capable of supporting Jumbo frame and LACP protocol.
8	Minimum shall be capable of supporting Fibre Channel (FC) or Internet Small Computer System Interface (iSCSI) connectivity on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
9	Shall provide the ability to expand iSCSI ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
10	Shall be capable of supporting native 10GbE host connections.
11	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
12	Solution shall support a minimum of 256 iSCSI initiators (host connections).

13	Minimum shall be capable of supporting Fibre Channel (FC) connectivity on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
14	Shall provide, excluding space on Storage System Operating System (OS) Drives, the initial data storage capacity must be distributed evenly among multiple shelves and support mirroring between shelves.
15	Shall provide the disk failure redundancy configuration to meet the capacity, IOPs and workload performance requirements (to be specified at delivery order level).
16	Shall provide the disk drive technologies to meet the capacity, IOPs and workload performance requirements (to be specified at delivery order level).
17	Shall provide capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
18	Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.
19	Shall provide a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
20	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
21	Shall provide a minimum of two storage controllers in a module for controller based storage solution, which are load balanced and provide automatic failover including the ability to maintain access to all data through a controller failure.
22	Shall provide the ability to upgrade a controller on the storage system without replacing the storage subsystem and the upgrade of the controller shall be non-destructive to the data, requiring no data migration, no reconfiguration and no LUN remapping to any connecting Host.

23	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
24	Shall provide the ability to expand and scale Host side connectivity and backend capacity, independently in order to increase performance.
25	Shall provide storage subsystem support boot from SAN.
26	Shall support the ability to manually change LUN UDID value.
27	Shall support the ability to create LUNs and volumes across multiple spindles.
28	Shall support non-disruptive LUN and volume expansion.
29	Shall support ability to present a minimum of a 15TB LUN/volume to a host.
30	Shall provide the ability to use "Thin Provisioning" or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
31	Shall provide that storage subsystem performance will not be affected when using "Thin Provisioning".
32	Shall provide the ability to expand Fibre Channel ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
33	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
34	Shall provide the capability of synchronous and asynchronous replication with write order fidelity.
35	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
36	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
37	Shall be capable of maintaining redundancy and the performance metrics requirements as stated above during snapshot and clone operations.
38	Power Switches shall be covered to prevent inadvertent activation.

39	Shall provide role-based security or audit trail logging for access to storage.
40	Shall provide a single master management interface to manage multiple storage subsystem of the same type in data center implementations.
41	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
42	Shall have a graphical user interface (GUI) or command (CLI), or a Wizard to automate the process to provision a large number of Disk Groups and LUNs.
43	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.
44	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.
45	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

High Performance SAN Storage	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support a minimum of 100,000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
2	Shall support minimum aggregate data rate of 7000 MBytes per second for all read or write or combination of read/write operations through the storage subsystem.
3	Shall provide the minimum usable native disk capacity of 75 TB without compression or deduplication.
4	Shall be capable of supporting a minimum of four (4) 8-Gbit/s Fibre Channel ports per controller. All Fibre Channel ports shall be capable of autosensing slower speeds of 2 and 4 Gbit/s.
5	Minimum shall be capable of supporting Fibre Channel (FC) connectivity on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
6	Shall provide in the case of a Frame storage solution, having a minimum of two storage backend ports/disk adapters in a module or a card that are load balanced and provide automatic failover between them.
7	Shall provide capability of isolating subsystem resources (Ports, Host I/F and Disk) and dedicate a defined amount of resources to a particular host.
8	Shall provide the native capability to monitor or maintain the IOPs requirements on individual applications running on the same storage subsystem. The monitoring is to ensure the performances of existing applications are not affected when new applications are added to the storage subsystem.
9	Shall provide the ability to allow source update during data migration. Online data migration from other storage array and data migration is transparent to users.

10	Shall provide, excluding space on Storage System Operating System (OS) Drives, the initial data storage capacity must be distributed evenly among multiple shelves and support mirroring between shelves.
11	Shall provide the disk failure redundancy configuration to meet the capacity, IOPs and workload performance requirements (to be specified at delivery order level).
12	Shall provide the disk drive technologies to meet the capacity, IOPs and workload performance requirements (to be specified at delivery order level).
13	Shall provide capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
14	Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.
15	Shall provide a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
16	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
17	Shall provide a minimum of two storage controllers in a module for controller based storage solution, which are load balanced and provide automatic failover including the ability to maintain access to all data through a controller failure.
18	Shall provide the ability to upgrade a controller on the storage system without replacing the storage subsystem and the upgrade of the controller shall be non-destructive to the data, requiring no data migration, no reconfiguration and no LUN remapping to any connecting Host.
19	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.

20	Shall provide the ability to expand and scale Host side connectivity and backend capacity, independently in order to increase performance.
21	Shall provide storage subsystem support boot from SAN.
22	Shall support the ability to manually change LUN UDID value.
23	Shall support the ability to create LUNs and volumes across multiple spindles.
24	Shall support non-disruptive LUN and volume expansion.
25	Shall support ability to present a minimum of a 15TB LUN/volume to a host.
26	Shall provide the ability to use “Thin Provisioning” or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
27	Shall provide that storage subsystem performance will not be affected when using “Thin Provisioning”.
28	Shall provide the ability to expand Fibre Channel ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
29	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
30	Shall provide the capability of synchronous and asynchronous replication with write order fidelity.
31	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
32	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
33	Shall be capable of maintaining redundancy and the performance metrics requirements as stated above during snapshot and clone operations.
34	Power Switches shall be covered to prevent inadvertent activation.
35	Shall provide role-based security or audit trail logging for access to storage.
36	Shall provide a single master management interface to manage multiple storage subsystem of the same type in data center implementations.

37	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
38	Shall have a graphical user interface (GUI) or command (CLI), or a Wizard to automate the process to provision a large number of Disk Groups and LUNs.
39	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.
40	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.
41	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

Fibre Fabric SAN Switch - Small to Medium	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall provide support for a minimum of 96 FC (Fiber Channel) ports in a single chassis (switch enclosure).
2	Shall provide support for Fiber Channel Protocol, minimum port speed will be 8 Gbit/s Fiber Channel Ports and all Fibre Channel ports shall be capable of autosensing slower speeds.
3	Shall support a minimum of 256 Gbit/per second of internal bandwidth in a single chassis (switch enclosure).
4	Shall support no more than 4:1 over subscription at 8 Gbit/per second.
5	Shall support N Port Virtualization with NPV or similar technology.
6	Shall provide Redundant Fabric Connectivity between Hosts and Storage device.
7	Shall provide Redundant Switch Control (Supervisor) Cards.
8	Shall provide redundancy in all switch components with no single point of failure and non-disruptive to operations for all switch component replacements or repairs or firmware and microcode upgrades or updates.
9	Solution shall provide that all components be easily accessible without having to de-install, disconnect or remove other components so that service can be accomplished without interruption to normal switch operations.
10	Shall provide Fabric Isolation, Local SAN Fabric shall be isolated from replication SAN Fabric.
11	Shall provide the ability to isolate data path from Host to Storage within a fabric, and configure throughput for specific applications.
12	Solution shall be able to provision additional Fibre ports required to fully connect solution components (storage subsystems, inter-switch links, management hosts, replication hardware, etc) in addition to host(s) without interruption to normal operations.

13	Shall provide fully redundant configuration, shall have the ability to retain a copy of the current configuration and the previous configuration.
14	Solution shall provide cover to all power switches to prevent inadvertent activation.
15	Shall support ability to be managed from a single Fabric management tool which can access all components in the SAN Fabric switch.
16	Shall provide the support of role-based security for access and management of the switch.
17	Shall support authenticable access with logging (for audits).
18	Solution shall provide a single sign-on integrated with Microsoft Active Directory (AD) or LDAP to manage Fabric(s) in a data center implementation from a single master management console.
19	Shall provide the ability to gather performance statistics for Inter-Switch Links (ISLs), host and storage device connections, and traffic between specific Fiber Channel sources and destinations (flows).
20	Shall provide the ability to set performance thresholds based on manual entry or calculated based on previous measurements.
21	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential switch system problems, failures and switch resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
22	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Fabric Switch Subsystem, such as switch cards, ports, ports GBICs, Fans or Power Supplies and similar components.
23	Shall provide a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

Fibre Fabric SAN Switch - Large	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall provide support for a minimum of 288 FC (Fiber Channel) ports in a single chassis (switch enclosure).
2	Shall provide support for Fiber Channel Protocol, minimum port speed will be 8 Gbit/s Fiber Channel Ports and all Fibre Channel ports shall be capable of autosensing slower speeds.
3	Shall support a minimum of 256 Gbit/per second of internal bandwidth in a single chassis (switch enclosure).
4	Shall support no more than 4:1 over subscription at 8 Gbit/per second.
5	Shall support N Port Virtualization with NPV or similar technology.
6	Shall provide Redundant Fabric Connectivity between Hosts and Storage device.
7	Shall provide Redundant Switch Control (Supervisor) Cards.
8	Shall provide redundancy in all switch components with no single point of failure and non-disruptive to operations for all switch component replacements or repairs or firmware and microcode upgrades or updates.
9	Solution shall provide that all components be easily accessible without having to de-install, disconnect or remove other components so that service can be accomplished without interruption to normal switch operations.
10	Shall provide Fabric Isolation, Local SAN Fabric shall be isolated from replication SAN Fabric.
11	Shall provide the ability to isolate data path from Host to Storage within a fabric, and configure throughput for specific applications.
12	Solution shall be able to provision additional Fibre ports required to fully connect solution components (storage subsystems, inter-switch links, management hosts, replication hardware, etc) in addition to host(s) without interruption to normal operations.

13	Shall provide fully redundant configuration, shall have the ability to retain a copy of the current configuration and the previous configuration.
14	Solution shall provide cover to all power switches to prevent inadvertent activation.
15	Shall support ability to be managed from a single Fabric management tool which can access all components in the SAN Fabric switch.
16	Shall provide the support of role-based security for access and management of the switch.
17	Shall support authenticable access with logging (for audits).
18	Solution shall provide a single sign-on integrated with Microsoft Active Directory (AD) or LDAP to manage Fabric(s) in a data center implementation from a single master management console.
19	Shall provide the ability to gather performance statistics for Inter-Switch Links (ISLs), host and storage device connections, and traffic between specific Fiber Channel sources and destinations (flows).
20	Shall provide the ability to set performance thresholds based on manual entry or calculated based on previous measurements.
21	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential switch system problems, failures and switch resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
22	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Fabric Switch Subsystem, such as switch cards, ports, ports GBICs, Fans or Power Supplies and similar components.
23	Shall provide a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

Low Performance NAS Storage	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support a minimum of 15000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
2	Shall support minimum of 1000 MBytes per second throughput.
3	Shall provide the minimum usable disk capacity of 25 TB . This initial data storage capacity must be distributed evenly among two or more shelves in order for future local mirroring between shelves.
4	Shall be capable of supporting a minimum of two (2) 1GbE Ethernet ports per controller.
5	Shall be capable of supporting a minimum of one (1) 10GbE Ethernet ports per controller.
6	Shall provide, excluding space on Storage System Operating System (OS) Drives, the initial data storage capacity must be distributed evenly among multiple shelves and support mirroring between shelves.
7	Shall provide the disk failure redundancy configuration to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
8	Shall provide the appropriate disk drive technologies to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
9	Shall provide the capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
10	Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.

11	Shall provide a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
12	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
13	Shall provide having a minimum of two storage controllers in a module for controller based storage solution, which are load balanced and provide automatic failover including the ability to maintain access to all data through a controller failure.
14	Shall provide the ability to upgrade a controller on the storage system without replacing the storage subsystem. The upgrade of the controller shall be non-destructive to the data, requiring no data migration, no reconfiguration and no LUN remapping to any connecting Host.
15	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
16	Shall provide the ability to expand and scale Host side connectivity and backend capacity independently in order to increase performance.
17	Shall support the ability to create volumes across multiple spindles.
18	Shall support dynamic volume expansion.
19	Shall be able to present a minimum of 15TB volume to connecting hosts.
20	Shall provide ability to use "Thin Provisioning" or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
21	Shall provide that storage subsystem performance will not be affected when using "Thin Provisioning".
22	Shall provide the capability of supporting Network File System (NFS) v4 or Higher, and Common Internet File System (CIFS) connectivity simultaneously on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
23	Shall be capable of supporting Jumbo frame and LACP protocol.

24	Shall provide the ability to expand Ethernet ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
25	Shall be capable of supporting 10GbE Ethernet ports.
26	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
27	Shall provide the capability of asynchronous replication.
28	Shall provide the maintaining redundancy and performance metrics requirements as stated above during snapshot and clone operations.
29	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times.
30	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times.
31	Shall provide the ability to allow source update during data migration. Online data migration from other storage devices and data migration is transparent to users.
32	Power Switches shall be covered to prevent inadvertent activation.
33	Shall support role-based security or audit trail logging for access to storage.
34	Shall provide a single master management interface to manage multiple storage subsystems of the same type in data center implementations.
35	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
36	Shall have a graphical user interface (GUI) or command line interface (CLI), or a Wizard to automate the process to provision a large number of Disk Groups or Volumes.
37	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.

38	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.
39	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

Medium Performance NAS Storage	
OEM Model/Part Number:	
Reference Number	Requirements
	1 Shall support a minimum of 35000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
	2 Shall support minimum of 2500 MBytes per second throughput.
	3 Shall provide the minimum usable disk capacity of 50 TB . This initial data storage capacity must be distributed evenly among two or more shelves in order for future local mirroring between shelves.
	4 Shall be capable of supporting a minimum of four (4) 1GbE Ethernet ports per controller.
	5 Shall be capable of supporting a minimum of two (2) 10GbE Ethernet ports per controller.
	6 Shall provide, excluding space on Storage System Operating System (OS) Drives, the initial data storage capacity must be distributed evenly among multiple shelves and support mirroring between shelves.
	7 Shall provide the disk failure redundancy configuration to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
	8 Shall provide the appropriate disk drive technologies to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
	9 Shall provide the capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
	10 Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.

11	Shall provide a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
12	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
13	Shall provide having a minimum of two storage controllers in a module for controller based storage solution, which are load balanced and provide automatic failover including the ability to maintain access to all data through a controller failure.
14	Shall provide the ability to upgrade a controller on the storage system without replacing the storage subsystem. The upgrade of the controller shall be non-destructive to the data, requiring no data migration, no reconfiguration and no LUN remapping to any connecting Host.
15	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
16	Shall provide the ability to expand and scale Host side connectivity and backend capacity independently in order to increase performance.
17	Shall support the ability to create volumes across multiple spindles.
18	Shall support dynamic volume expansion.
19	Shall be able to present a minimum of 15TB volume to connecting hosts.
20	Shall provide ability to use "Thin Provisioning" or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
21	Shall provide that storage subsystem performance will not be affected when using "Thin Provisioning".
22	Shall provide the capability of supporting Network File System (NFS) v4 or Higher, and Common Internet File System (CIFS) connectivity simultaneously on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
23	Shall be capable of supporting Jumbo frame and LACP protocol.

24	Shall provide the ability to expand Ethernet ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
25	Shall be capable of supporting 10GbE Ethernet ports.
26	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
27	Shall provide the capability of asynchronous replication.
28	Shall provide the maintaining redundancy and performance metrics requirements as stated above during snapshot and clone operations.
29	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times.
30	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times.
31	Shall provide the ability to allow source update during data migration. Online data migration from other storage devices and data migration is transparent to users.
32	Power Switches shall be covered to prevent inadvertent activation.
33	Shall support role-based security or audit trail logging for access to storage.
34	Shall provide a single master management interface to manage multiple storage subsystems of the same type in data center implementations.
35	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
36	Shall have a graphical user interface (GUI) or command line interface (CLI), or a Wizard to automate the process to provision a large number of Disk Groups or Volumes.
37	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.

38	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.
39	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

High Performance NAS Storage	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support a minimum of 75000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
2	Shall support minimum of 4000 MBytes per second throughput.
3	Shall provide the minimum usable disk capacity of 75 TB . This initial data storage capacity must be distributed evenly among two or more shelves in order for future local mirroring between shelves.
4	Shall be capable of supporting a minimum of four (4) 1GbE Ethernet ports per controller.
5	Shall be capable of supporting a minimum of two (2) 10GbE Ethernet ports per controller.
6	Shall provide, excluding space on Storage System Operating System (OS) Drives, the initial data storage capacity must be distributed evenly among multiple shelves and support mirroring between shelves.
7	Shall provide the disk failure redundancy configuration to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
8	Shall provide the appropriate disk drive technologies to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
9	Shall provide the capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
10	Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.

11	Shall provide a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
12	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
13	Shall provide having a minimum of two storage controllers in a module for controller based storage solution, which are load balanced and provide automatic failover including the ability to maintain access to all data through a controller failure.
14	Shall provide the ability to upgrade a controller on the storage system without replacing the storage subsystem. The upgrade of the controller shall be non-destructive to the data, requiring no data migration, no reconfiguration and no LUN remapping to any connecting Host.
15	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
16	Shall provide the ability to expand and scale Host side connectivity and backend capacity independently in order to increase performance.
17	Shall support the ability to create volumes across multiple spindles.
18	Shall support dynamic volume expansion.
19	Shall be able to present a minimum of 15TB volume to connecting hosts.
20	Shall provide ability to use "Thin Provisioning" or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
21	Shall provide that storage subsystem performance will not be affected when using "Thin Provisioning".
22	Shall provide the capability of supporting Network File System (NFS) v4 or Higher, and Common Internet File System (CIFS) connectivity simultaneously on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
23	Shall be capable of supporting Jumbo frame and LACP protocol.

24	Shall provide the ability to expand Ethernet ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
25	Shall be capable of supporting 10GbE Ethernet ports.
26	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
27	Shall provide the capability of asynchronous replication.
28	Shall provide the maintaining redundancy and performance metrics requirements as stated above during snapshot and clone operations.
29	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times.
30	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times.
31	Shall provide the ability to allow source update during data migration. Online data migration from other storage devices and data migration is transparent to users.
32	Power Switches shall be covered to prevent inadvertent activation.
33	Shall support role-based security or audit trail logging for access to storage.
34	Shall provide a single master management interface to manage multiple storage subsystems of the same type in data center implementations.
35	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
36	Shall have a graphical user interface (GUI) or command line interface (CLI), or a Wizard to automate the process to provision a large number of Disk Groups or Volumes.
37	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.

38	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.
39	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

Low Performance NAS Storage Modular	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support a minimum of 15000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
2	Shall support minimum of 1000 MBytes per second throughput.
3	Shall provide the minimum usable disk capacity of 25 TB . This initial data storage capacity must be distributed evenly among two or more shelves in order for future local mirroring between shelves.
4	Shall be capable of supporting a minimum of two (2) 1GbE Ethernet ports per controller.
5	Shall be capable of supporting a minimum of one (1) 10GbE Ethernet ports per controller.
6	Shall provide the disk failure redundancy configuration to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
7	Shall provide the appropriate disk drive technologies to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
8	Shall provide the capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
9	Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.
10	Shall Support a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
11	Shall natively provide Single Global Namespace file system from the storage device.

12	Shall provide the capability of maintaining Single Global Namespace within the Data Center when scale beyond the maximum capacity of the storage device.
13	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
14	Shall provide having a minimum of two storage controllers or nodes in a subsystem that are load balanced and provide automatic failover including the ability to maintain access to all data through a controller or node failure.
15	Shall provide adding, upgrading or replacing storage subsystem components while adhering to the required storage subsystem uptime requirement, redundancy and needing no data migration, no reconfiguration and no LUN remapping to any connecting Host.
16	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
17	Shall provide the ability to expand and scale Host side connectivity and backend capacity independently in order to increase performance.
18	Shall support the ability to create volumes across multiple spindles.
19	Shall support dynamic volume expansion.
20	Shall provide ability to use "Thin Provisioning" or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
21	Shall provide that storage subsystem performance will not be affected when using "Thin Provisioning".
22	Shall provide the capability of supporting Network File System (NFS) v4 or Higher, and Common Internet File System (CIFS) connectivity simultaneously on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
23	Shall be capable of supporting Jumbo frame and LACP protocol.
24	Shall provide the ability to expand Ethernet ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
25	Shall be capable of supporting 10GbE Ethernet ports.

26	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
27	Shall provide the capability of asynchronous replication.
28	Shall be capable of maintaining redundancy and the performance metrics requirements as stated above during snapshot and clone operations.
29	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all time during the migration process.
30	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
31	Shall provide the ability to allow source update during data migration. Online data migration from other storage devices and data migration is transparent to users.
32	Power Switches shall be covered to prevent inadvertent activation.
33	Shall support role-based security or audit trail logging for access to storage.
34	Shall provide a single master management interface to manage multiple storage subsystems of the same type in data center implementations.
35	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
36	Shall have a graphical user interface (GUI) or command line interface (CLI), or a Wizard to automate the process to provision a large number of Disk Groups or Volumes.
37	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.
38	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.

39	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.
----	--

Medium Performance NAS Storage Modular	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support a minimum of 35000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
2	Shall support minimum of 2500 MBytes per second throughput.
3	Shall provide the minimum usable disk capacity of 50 TB . This initial data storage capacity must be distributed evenly among two or more shelves in order for future local mirroring between shelves.
4	Shall be capable of supporting a minimum of four (4) 1GbE Ethernet ports per controller.
5	Shall be capable of supporting a minimum of two (2) 10GbE Ethernet ports per controller.
6	Shall provide the disk failure redundancy configuration to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
7	Shall provide the appropriate disk drive technologies to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
8	Shall provide the capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
9	Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.
10	Shall Support a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
11	Shall natively provide Single Global Namespace file system from the storage device.

12	Shall provide the capability of maintaining Single Global Namespace within the Data Center when scale beyond the maximum capacity of the storage device.
13	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
14	Shall provide having a minimum of two storage controllers or nodes in a subsystem that are load balanced and provide automatic failover including the ability to maintain access to all data through a controller or node failure.
15	Shall provide adding, upgrading or replacing storage subsystem components while adhering to the required storage subsystem uptime requirement, redundancy and needing no data migration, no reconfiguration and no LUN remapping to any connecting Host.
16	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
17	Shall provide the ability to expand and scale Host side connectivity and backend capacity independently in order to increase performance.
18	Shall support the ability to create volumes across multiple spindles.
19	Shall support dynamic volume expansion.
20	Shall provide ability to use "Thin Provisioning" or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
21	Shall provide that storage subsystem performance will not be affected when using "Thin Provisioning".
22	Shall provide the capability of supporting Network File System (NFS) v4 or Higher, and Common Internet File System (CIFS) connectivity simultaneously on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
23	Shall be capable of supporting Jumbo frame and LACP protocol.
24	Shall provide the ability to expand Ethernet ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
25	Shall be capable of supporting 10GbE Ethernet ports.

26	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
27	Shall provide the capability of asynchronous replication.
28	Shall be capable of maintaining redundancy and the performance metrics requirements as stated above during snapshot and clone operations.
29	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all time during the migration process.
30	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
31	Shall provide the ability to allow source update during data migration. Online data migration from other storage devices and data migration is transparent to users.
32	Power Switches shall be covered to prevent inadvertent activation.
33	Shall support role-based security or audit trail logging for access to storage.
34	Shall provide a single master management interface to manage multiple storage subsystems of the same type in data center implementations.
35	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
36	Shall have a graphical user interface (GUI) or command line interface (CLI), or a Wizard to automate the process to provision a large number of Disk Groups or Volumes.
37	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.
38	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.

39	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.
----	--

High Performance NAS Storage Modular	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support a minimum of 75000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
2	Shall support minimum of 4000 MBytes per second throughput.
3	Shall provide the minimum usable disk capacity of 75 TB . This initial data storage capacity must be distributed evenly among two or more shelves in order for future local mirroring between shelves.
4	Shall be capable of supporting a minimum of four (4) 1GbE Ethernet ports per controller.
5	Shall be capable of supporting a minimum of two (2) 10GbE Ethernet ports per controller.
6	Shall provide the disk failure redundancy configuration to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
7	Shall provide the appropriate disk drive technologies to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
8	Shall provide the capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
9	Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.
10	Shall Support a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
11	Shall natively provide Single Global Namespace file system from the storage device.

12	Shall provide the capability of maintaining Single Global Namespace within the Data Center when scale beyond the maximum capacity of the storage device.
13	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
14	Shall provide having a minimum of two storage controllers or nodes in a subsystem that are load balanced and provide automatic failover including the ability to maintain access to all data through a controller or node failure.
15	Shall provide adding, upgrading or replacing storage subsystem components while adhering to the required storage subsystem uptime requirement, redundancy and needing no data migration, no reconfiguration and no LUN remapping to any connecting Host.
16	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
17	Shall provide the ability to expand and scale Host side connectivity and backend capacity independently in order to increase performance.
18	Shall support the ability to create volumes across multiple spindles.
19	Shall support dynamic volume expansion.
20	Shall provide ability to use "Thin Provisioning" or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
21	Shall provide that storage subsystem performance will not be affected when using "Thin Provisioning".
22	Shall provide the capability of supporting Network File System (NFS) v4 or Higher, and Common Internet File System (CIFS) connectivity simultaneously on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
23	Shall be capable of supporting Jumbo frame and LACP protocol.
24	Shall provide the ability to expand Ethernet ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
25	Shall be capable of supporting 10GbE Ethernet ports.

26	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
27	Shall provide the capability of asynchronous replication.
28	Shall be capable of maintaining redundancy and the performance metrics requirements as stated above during snapshot and clone operations.
29	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all time during the migration process.
30	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
31	Shall provide the ability to allow source update during data migration. Online data migration from other storage devices and data migration is transparent to users.
32	Power Switches shall be covered to prevent inadvertent activation.
33	Shall support role-based security or audit trail logging for access to storage.
34	Shall provide a single master management interface to manage multiple storage subsystems of the same type in data center implementations.
35	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
36	Shall have a graphical user interface (GUI) or command line interface (CLI), or a Wizard to automate the process to provision a large number of Disk Groups or Volumes.
37	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.
38	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.

39	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.
----	--

Low Performance iSCSI Storage Modular	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support a minimum of 20000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
2	Shall support minimum of 1000 MBytes per second throughput.
3	Shall provide the minimum usable disk capacity of 25 TB . This initial data storage capacity must be distributed evenly among two or more shelves in order for future local mirroring between shelves.
4	Shall be capable of supporting a minimum of two (2) 1GbE iSCSI ports per controller.
5	Shall be capable of supporting a minimum of one (1) 10GbE iSCSI ports per controller.
6	Shall provide the disk failure redundancy configuration to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
7	Shall provide the appropriate disk drive technologies to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
8	Shall provide capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
9	Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.
10	Shall provide a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).

11	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode. upgrades or updates.
12	Shall provide having a minimum of two storage controllers in a module for controller based storage solutions or a node, which are load balanced and provide automatic failover including the ability to maintain access to all data through a controller failure.
13	Shall provide the ability to upgrade a controller or a node on the storage system without replacing the storage subsystem and the upgrade of the controller or the node, shall be non-destructive to the data, requiring no data migration, no reconfiguration and no LUN remapping to any connecting Host.
14	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
15	Shall provide the ability to expand and scale Host side connectivity and backend capacity independently in order to increase performance.
16	Shall provide storage subsystem support boot from SAN.
17	Shall support the ability to manually change LUN UDID value.
18	Shall support the ability to create volumes across multiple spindles.
19	Shall support non-disruptive LUN and volume expansion.
20	Shall be able to present a minimum of 15TB LUN/volume to a host via iSCSI.
21	Shall provide the ability to use "Thin Provisioning" or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
22	Shall provide that storage subsystem performance will not be affected when using "Thin Provisioning".
23	Minimum shall be capable of supporting Internet Small Computer System Interface (iSCSI) connectivity on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
24	Shall support the ability to expand iSCSI ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
25	Shall be capable of supporting 10GbE Ethernet ports.

26	Shall be capable of supporting Jumbo frame and LACP protocol.
27	Solution shall support a minimum of 256 SCSI initiators (host connections).
28	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
29	Shall provide the capability of synchronous and asynchronous replication with write order fidelity.
30	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
31	Solution shall be able to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
32	Shall be able to allow source update during data migration. Online data migration from other storage array and data migration is transparent to users.
33	Shall be capable of maintaining redundancy and the performance metrics requirements as stated above during snapshot and clone operations.
34	Power Switches shall be covered to prevent inadvertent activation.
35	Shall support role-based security or audit trail logging for access to storage.
36	Shall provide a single master management interface to manage multiple storage subsystems of the same type in data center implementations.
37	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
38	Shall have a graphical user interface (GUI) or command (CLI), or a Wizard to automate the process to provision a large number of Disk Groups and LUNs.
39	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.

40	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.
41	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar function.

Medium Performance iSCSI Storage Modular	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support a minimum of 50000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
2	Shall support minimum of 2500 MBytes per second throughput.
3	Shall provide the minimum usable disk capacity of 50 TB . This initial data storage capacity must be distributed evenly among two or more shelves in order for future local mirroring between shelves.
4	Shall be capable of supporting a minimum of four (4) 1GbE iSCSI ports per controller.
5	Shall be capable of supporting a minimum of two (2) 10GbE iSCSI ports per controller.
6	Shall provide the disk failure redundancy configuration to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
7	Shall provide the appropriate disk drive technologies to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
8	Shall provide capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
9	Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.
10	Shall provide a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).

11	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode. upgrades or updates.
12	Shall provide having a minimum of two storage controllers in a module for controller based storage solutions or a node, which are load balanced and provide automatic failover including the ability to maintain access to all data through a controller failure.
13	Shall provide the ability to upgrade a controller or a node on the storage system without replacing the storage subsystem and the upgrade of the controller or the node, shall be non-destructive to the data, requiring no data migration, no reconfiguration and no LUN remapping to any connecting Host.
14	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
15	Shall provide the ability to expand and scale Host side connectivity and backend capacity independently in order to increase performance.
16	Shall provide storage subsystem support boot from SAN.
17	Shall support the ability to manually change LUN UDID value.
18	Shall support the ability to create volumes across multiple spindles.
19	Shall support non-disruptive LUN and volume expansion.
20	Shall be able to present a minimum of 15TB LUN/volume to a host via iSCSI.
21	Shall provide the ability to use "Thin Provisioning" or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
22	Shall provide that storage subsystem performance will not be affected when using "Thin Provisioning".
23	Minimum shall be capable of supporting Internet Small Computer System Interface (iSCSI) connectivity on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
24	Shall support the ability to expand iSCSI ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
25	Shall be capable of supporting 10GbE Ethernet ports.

26	Shall be capable of supporting Jumbo frame and LACP protocol.
27	Solution shall support a minimum of 256 SCSI initiators (host connections).
28	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
29	Shall provide the capability of synchronous and asynchronous replication with write order fidelity.
30	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
31	Solution shall be able to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
32	Shall be able to allow source update during data migration. Online data migration from other storage array and data migration is transparent to users.
33	Shall be capable of maintaining redundancy and the performance metrics requirements as stated above during snapshot and clone operations.
34	Power Switches shall be covered to prevent inadvertent activation.
35	Shall support role-based security or audit trail logging for access to storage.
36	Shall provide a single master management interface to manage multiple storage subsystems of the same type in data center implementations.
37	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
38	Shall have a graphical user interface (GUI) or command (CLI), or a Wizard to automate the process to provision a large number of Disk Groups and LUNs.
39	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.

40	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.
41	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar function.

High Performance iSCSI Storage Modular	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support a minimum of 75000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
2	Shall support minimum of 4000 MBytes per second throughput.
3	Shall provide the minimum usable disk capacity of 75 TB . This initial data storage capacity must be distributed evenly among two or more shelves in order for future local mirroring between shelves.
4	Shall be capable of supporting a minimum of four (4) 1GbE iSCSI ports per controller.
5	Shall be capable of supporting a minimum of two (2) 10GbE iSCSI ports per controller.
6	Shall provide the disk failure redundancy configuration to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
7	Shall provide the appropriate disk drive technologies to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
8	Shall provide capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
9	Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.
10	Shall provide a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).

11	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode. upgrades or updates.
12	Shall provide having a minimum of two storage controllers in a module for controller based storage solutions or a node, which are load balanced and provide automatic failover including the ability to maintain access to all data through a controller failure.
13	Shall provide the ability to upgrade a controller or a node on the storage system without replacing the storage subsystem and the upgrade of the controller or the node, shall be non-destructive to the data, requiring no data migration, no reconfiguration and no LUN remapping to any connecting Host.
14	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
15	Shall provide the ability to expand and scale Host side connectivity and backend capacity independently in order to increase performance.
16	Shall provide storage subsystem support boot from SAN.
17	Shall support the ability to manually change LUN UDID value.
18	Shall support the ability to create volumes across multiple spindles.
19	Shall support non-disruptive LUN and volume expansion.
20	Shall be able to present a minimum of 15TB LUN/volume to a host via iSCSI.
21	Shall provide the ability to use "Thin Provisioning" or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
22	Shall provide that storage subsystem performance will not be affected when using "Thin Provisioning".
23	Minimum shall be capable of supporting Internet Small Computer System Interface (iSCSI) connectivity on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
24	Shall support the ability to expand iSCSI ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
25	Shall be capable of supporting 10GbE Ethernet ports.

26	Shall be capable of supporting Jumbo frame and LACP protocol.
27	Solution shall support a minimum of 256 SCSI initiators (host connections).
28	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
29	Shall provide the capability of synchronous and asynchronous replication with write order fidelity.
30	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
31	Solution shall be able to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
32	Shall be able to allow source update during data migration. Online data migration from other storage array and data migration is transparent to users.
33	Shall be capable of maintaining redundancy and the performance metrics requirements as stated above during snapshot and clone operations.
34	Power Switches shall be covered to prevent inadvertent activation.
35	Shall support role-based security or audit trail logging for access to storage.
36	Shall provide a single master management interface to manage multiple storage subsystems of the same type in data center implementations.
37	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
38	Shall have a graphical user interface (GUI) or command (CLI), or a Wizard to automate the process to provision a large number of Disk Groups and LUNs.
39	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.

40	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.
41	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar function.

	LTO Tape Library Large
	OEM Model/Part Number:
Reference Number	Requirements
1	Shall support the following minimum amount of storage that will be leveraging Long Term Storage of: 75 TB (Terabytes)
2	Shall support a minimum of 8 Tape Drives.
3	Shall support the ability to scale to at least 32 Tape Drives.
4	Shall support a minimum of 120 Tape Cartridge slots.
5	Shall support the ability to scale to at least 640 Tape Cartridge slots.
6	Shall provide a minimum of four (4) 8-Gbit/per second Fiber Channel ports per Library I/O Control Unit and all Fiber Channel ports shall be capable of autosensing slower speeds.
7	Shall provide a minimum of four (4) 1GbE ports for iSCSI to Fiber Channel Bridge Device or similar unit type (will be indicated as part of Delivery Order requirements if needed).
8	Shall support the connectivity of iSCSI to Fibre Channel bridge device or similar unit type (applies only to Reference #7 when needed and if indicated on Delivery Order).
9	Shall support the capability of a minimum throughput of 6 TB (Terabytes) per hour.
10	Shall support the capability of a minimum scalability of up to 24 TB (Terabytes) per hour.
11	Shall support LTO Ultrium (Linear Tape-Open) tape technology format.
12	Shall provide the appropriate Robotic access time to meet the stated IOPs and workload performance requirements (to be specified at delivery order level).
13	Shall provide Tape Drive to read and write to either LTO4 or higher specifications and throughput of 120 MB/s (Megabytes) or higher.
14	Shall provide the capability of Tape Drive encryption with a minimum 1 TB (Terabyte) tape capacity and throughput minimum of 120 MB/s (Megabytes) with using a minimum encryption of FIPS 140-2

15	Shall provide the capability of Tape Library and LTO Tape Drives that can support enterprise tape encryption using a minimum of FIPS 140-2 validated encryption.
16	Shall provide tape drives that read previously written tapes in LTO format back 2 previous LTO generations (example: LTO 2 Tapes able to be read by LTO 4 Tape Drive).
17	Shall provide port expansion capability to meet storage performance requirements (to be specified at delivery order level) in the same unit(s) for the Library .
18	Shall provide Library Fiber Channel ports expansion to meet the storage performance requirements (to be specified at delivery order level) in the same unit(s). Capable of adding additional ports per Library I/O Control Unit.
19	Tape Library shall be capable of supporting minimum of native 1GbE Ethernet or above host connectivity.
20	Shall support a tape cartridge bulk load capacity of: 10
21	Shall support the capability of expansion and scalability, including Interface cards and capacity (Tape Drives & Cartridge Slots) independently with minimum of planned downtime of 2 hours or less.
22	Shall support an automated and manual method to check Tape Drive and Robotic integrity.
23	Shall support the ability of the Library to recover from a Tape Drive failure and will not cause data loss.
24	Shall support the capability of multiple SCSI initiators (host connections) to the Library .
25	Shall Support a minimum of four nines storage subsystem uptime (or 99.99% availability, excluding planned downtime). (Note: Four Nines (99.99%) = 53 minutes of downtime on a rolling 12 month basis).
26	Shall support Tape Library having a minimum of two I/O Control Units/Board(s)/Card(s).
27	Shall provide redundancy in all Tape Library system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates (only exception is Library Robotic Arm). For firmware and microcode upgrades or updates only, maximum of two hour of planned maintenance time per year is allowed.

28	Shall support the capability of isolating subsystem resources (Ports, Interface Cards, and Tape Drives) and dedicate a defined amount of these resources to a particular host or VLAN.
29	Power switches shall be covered to prevent inadvertent activation.
30	Shall support role-based security for access and manage Tape Library control.
31	Shall support authenticable access with logging (for audits).
32	Shall support a single master management interface to manage multiple Tape Library(s) of the same type in data center implementations.
33	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage Tape Libraries in a data center implementation from a single master management console.
34	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential Tape Library system problems, failures and Library resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
35	Shall provide native capability to report and generate reports at a minimum on hardware failures or items out-of-specifications in the Tape Library & Subsystems, such as Tape Drives, Fans or Power Supplies and similar components.
36	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

LTO Tape Library Medium to Small	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support the following minimum amount of storage that will be leveraging Long Term Storage of: 25 TB (Terabytes).
2	Shall support a minimum of 4 Tape Drives.
3	Shall support the ability to scale to a maximum of 12 Tape Drives.
4	Shall support a minimum of 25 Tape Cartridge slots.
5	Shall support the ability to scale to a maximum of 180 Tape Cartridge slots.
6	Shall provide a minimum of two (2) 8-Gbit/second Fiber Channel ports per Library I/O Control Unit and all Fiber Channel ports shall be capable of autosensing slower speeds.
7	Shall provide a minimum of two (2) 1GbE ports for iSCSI to Fiber Channel Bridge Device or similar unit type (will be indicated as part of Delivery Order requirements if needed).
8	Shall support the connectivity of iSCSI to Fibre Channel bridge device or similar unit type (applies only to Reference #7 when needed and if indicated on Delivery Order).
9	Shall support the capability of a minimum throughput of 6 TB (Terabytes) per hour.
10	Shall support the capability of a minimum scalability of up to 12 TB (Terabytes) per hour.
11	Shall support LTO Ultrium (Linear Tape-Open) tape technology format.
12	Shall provide the appropriate Robotic access time to meet the stated IOPs and workload performance requirements (to be specified at delivery order level).
13	Shall provide Tape Drive to read and write to either LTO4 or higher specifications and throughput of 120 MB/s (Megabytes) or higher.

14	Shall provide the capability of Tape Drive encryption with a minimum 1 TB (Terabyte) tape capacity and throughput minimum of 120 MB/s (Megabytes) with using a minimum encryption of FIPS 140-2
15	Shall provide the capability of Tape Library and LTO Tape Drives that can support enterprise tape encryption using a minimum of FIPS 140-2 validated encryption.
16	Shall provide tape drives that read previously written tapes in LTO format back 2 previous LTO generations (example: LTO 2 Tapes able to be read by LTO 4 Tape Drive).
17	Shall provide port expansion capability to meet storage performance requirements (to be specified at delivery order level) in the same unit(s) for the Library .
18	Shall provide Library Fiber Channel ports expansion to meet the storage performance requirements (to be specified at delivery order level) in the same unit(s). Capable of adding additional ports per Library I/O Control Unit.
19	Tape Library shall be capable of supporting minimum of native 1GbE Ethernet or above host connectivity.
20	Shall support a tape cartridge bulk load capacity of: 10
21	Shall support the capability of expansion and scalability, including Interface cards and capacity (Tape Drives & Cartridge Slots) independently with minimum of planned downtime of 2 hours or less.
22	Shall support an automated and manual method to check Tape Drive and Robotic integrity.
23	Shall support the ability of the Library to recover from a Tape Drive failure and will not cause data loss.
24	Shall support the capability of multiple iSCSI initiators (host connections) to the Library .
25	Shall Support a minimum of four nines storage subsystem uptime (or 99.99% availability, excluding planned downtime). (Note: Four Nines (99.99%) = 53 minutes of downtime on a rolling 12 month basis).
26	Shall support Tape Library having a minimum of two I/O Control Units/Board(s)/Card(s).

27	Shall provide redundancy in all Tape Library system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates (only exception is Library Robotic Arm). For firmware and microcode upgrades or updates only, maximum of two hour of planned maintenance time per year is allowed.
28	Shall support the capability of isolating subsystem resources (Ports, Interface Cards, and Tape Drives) and dedicate a defined amount of these resources to a particular host or VLAN.
29	Power switches shall be covered to prevent inadvertent activation.
30	Shall support role-based security for access and manage Tape Library control.
31	Shall support authenticable access with logging (for audits).
32	Shall support a single master management interface to manage multiple Tape Library(s) of the same type in data center implementations.
33	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage Tape Libraries in a data center implementation from a single master management console.
34	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential Tape Library system problems, failures and Library resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
35	Shall provide native capability to report and generate reports at a minimum on hardware failures or items out-of-specifications in the Tape Library & Subsystems, such as Tape Drives, Fans or Power Supplies and similar components.
36	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

LTO Tape Cartridge (LTO4)	
OEM Model/Part Number:	
Reference Number	Requirements
1	Ultrium (LTO) cartridge's container dimensions to be 102.0 x 105.4 x 21.5(mm).
2	Ultrium (LTO) tape dimensions within the cartridge container shall be an industry standard of half-inch (½ inch) wide tape.
3	LTO tape format shall be laid out in this manner, 4 wide data bands, sandwiched between 5 narrow servo bands.
4	LTO tape format shall be laid out on tape in the following order, 4 data bands x 11-20 wraps per head x 8 or 16 tracks per wrap.
5	Every LTO 1 / 2 / 3 cartridge shall contain a Cartridge Memory chip capable of containing 128 blocks of memory, each block containing 32 Bytes for a total of 4 KB.
6	Every LTO 4 / 5 cartridge shall contain a Cartridge Memory chip capable of containing 256 blocks of memory, each block containing 32 Bytes for a total of 8 KB.
7	Every LTO Cartridge Memory chip shall be capable of being read and/or written, one block at a time by a non contacting passive RF interface.
8	Every LTO Cartridge tape shall have a leader pin attached to the end of the tape to enable the tape drive to grasp the tape and mount it in a take-up reel inside the tape drive.
9	Every LTO Cartridge tape shall have this leader pin held in place at the opening of the tape cartridge by a small spring when the tape cartridge is not in a tape drive.
10	The LTO cartridge tape shall be capable of the following: 15-30 years of archival life. 5000 cartridge loads/unloads and approx. 260 full file passes.

11	LTO-4: Native Data Capacity 800GB; Compression Capability 2:1; Partition Capable=No; Tape Thickness=6.6 um; Tape Length=820 m; Tape Tracks=896; Wraps per Band=14; Linear Density (bits/mm)=13250
----	--

LTO Tape Cartridge (LTO5)	
OEM Model/Part Number:	
Reference Number	Requirements
1	Ultrium (LTO) cartridge's container dimensions to be 102.0 x 105.4 x 21.5(mm).
2	Ultrium (LTO) tape dimensions within the cartridge container shall be an industry standard of half-inch (½ inch) wide tape.
3	LTO tape format shall be laid out in this manner, 4 wide data bands, sandwiched between 5 narrow servo bands.
4	LTO tape format shall be laid out on tape in the following order, 4 data bands x 11-20 wraps per head x 8 or 16 tracks per wrap.
5	Every LTO 1 / 2 / 3 cartridge shall contain a Cartridge Memory chip capable of containing 128 blocks of memory, each block containing 32 Bytes for a total of 4 KB.
6	Every LTO 4 / 5 cartridge shall contain a Cartridge Memory chip capable of containing 256 blocks of memory, each block containing 32 Bytes for a total of 8 KB.
7	Every LTO Cartridge Memory chip shall be capable of being read and/or written, one block at a time by a non contacting passive RF interface.
8	Every LTO Cartridge tape shall have a leader pin attached to the end of the tape to enable the tape drive to grasp the tape and mount it in a take-up reel inside the tape drive.
9	Every LTO Cartridge tape shall have this leader pin held in place at the opening of the tape cartridge by a small spring when the tape cartridge is not in a tape drive.
10	The LTO cartridge tape shall be capable of the following: 15-30 years of archival life. 5000 cartridge loads/unloads and approx. 260 full file passes.

11	LTO-5: Native Data Capacity 1.5TB; Compression Capability 2:1; Partition Capable=Yes; Tape Thickness=6.4 um; Tape Length=846 m; Tape Tracks=1280; Wraps per Band=20; Linear Density (bits/mm)=15142
----	--

IP Based Deduplication Storage (Small)	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall provide the minimum usable native disk capacity without data compression, without data Deduplication, and without single instance (no duplicate objects) of up to 10TB (Terabytes), expandable to a maximum of 50TB (Terabytes).
2	Shall provide a minimum ingest aggregate throughput of 1.8TB/hr.
3	Solution shall support interoperability between different sized units (Extra large, Large, Medium, and Small)
4	Shall support concurrent parallel I/O streaming.
5	Solution shall provide the ability to support an IP based storage device that supports both Network File System (NFS)v3 or Higher, and Common Internet File System (CIFS) connectivity protocols. All connecting protocols shall support up to the maximum usable storage capacity of the device.
6	Solution shall provide a minimum of two 1GbE and Ethernet ports per system.
7	Solution shall provide a minimum of two 10GbE Ethernet ports per system.
8	Shall provide the support of Jumbo frame, LACP (802.3ad) protocol, and bandwidth aggregation.
9	Shall support Ethernet port expansion to meet storage performance requirements in the same unit(s) as listed above (to be specified at delivery order level) for each storage size types. Capable of adding minimum of two additional ports per system.

10	Solution shall provide storage capacity expansion or scalability with no downtime, no forklift upgrade, no reconfiguration of the internal operating system or re-creation of the existing subsystem components, and remapping connections of the storage subsystem to connecting hosts. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
11	Shall support expansion and scalability of the Data Deduplication System without requiring a forklift upgrade.
12	Shall support that Data residing on the Deduplication device that meets the requirement to replicate to a geo-dispersed environment (one to many).
13	Shall provide edge to core replication. Many to one replication.
14	Shall provide Deduplication on the hardware appliance, not as a software only solution.
15	Shall provide a fully redundant solution and support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
16	Shall provide fast instant restore of files and fast restore of a complete file system to primary storage and to tape without the need to rehydrate and reconstitute data on external or additional disk storage.
17	Shall integrate with _____ Enterprise backup software (to be specified at the delivery order level).
18	Shall provide the ability to be directly attached as a NAS device for a large block sequential I/O data stream.
19	Shall meet the requirement to have a portion of the storage for saving non-deduped data and another portion for deduped data.
20	Shall meet the requirement to select a portion of storage for data replication.
21	Shall provide a built-in capability of self healing that provides corruption recovery during replication.
22	Shall integrate with backup software to backup data directly to tape from the Deduplication secondary storage device.

23	Shall Support a minimum of four nines storage subsystem uptime (or 99.99% availability, excluding planned downtime). (Note: Four Nines (99.99%) = 53 minutes of downtime on a rolling 12 month basis).
24	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
25	Solution shall be able to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
26	Shall provide disk based data Deduplication.
27	Shall provide built-in capability of perform automatic data Integrity checking after data Deduplication.
28	Shall provide secure data Deduplication algorithms.
29	Shall provide built-in capability for self healing that provides corruption recovery when data corruption is detected after Deduplication, without Re-Deduplication of the original data again.
30	Shall provide the ability to rebuild file system from stored metadata.
31	Shall provide the ability to ingest data from multiple sources (from software and/or hardware) simultaneously.
32	Shall provide cover to power switches to prevent inadvertent activation.
33	Shall provide the support of role-based security for access and management of storage devices.
34	Shall support authenticable access with logging (for audits).
35	Shall support a native Management tool able to manage multiple Deduplication Storage devices of the same type in data center implementations.
36	Shall provide a single sign-on integrated with Microsoft Active Directory (AD) or LDAP to manage Deduplication Storage device(s) in a data center implementation from a single master Management console.

37	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
38	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and similar components.
39	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

IP Based Deduplication Storage (Medium)	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall provide the minimum usable native disk capacity without data compression, without data Deduplication, and without single instance (no duplicate objects) of 50TB (Terabytes), expandable to a maximum of 100TB (Terabytes).
2	Shall provide a minimum ingest aggregate throughput of 3TB/hr.
3	Solution shall support interoperability between different sized units (Extra large, Large, Medium, and Small)
4	Shall support concurrent parallel I/O streaming.
5	Solution shall provide the ability to support an IP based storage device that supports both Network File System (NFS) v3 or Higher, and Common Internet File System (CIFS) connectivity protocols. All connecting protocols shall support up to the maximum usable storage capacity of the device.
6	Solution shall provide a minimum of two 1GbE and Ethernet ports per system.
7	Solution shall provide a minimum of two 10GbE Ethernet ports per system.
8	Shall provide the support of Jumbo frame, LACP (802.3ad) protocol, and bandwidth aggregation.
9	Shall support Ethernet port expansion to meet storage performance requirements in the same unit(s) as listed above (to be specified at delivery order level) for each storage size types. Capable of adding minimum of two additional ports per system.

10	Solution shall provide storage capacity expansion or scalability with no downtime, no forklift upgrade, no reconfiguration of the internal operating system or re-creation of the existing subsystem components, and remapping connections of the storage subsystem to connecting hosts. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
11	Shall support expansion and scalability of the Data Deduplication System without requiring a forklift upgrade.
12	Shall support that Data residing on the Deduplication device that meets the requirement to replicate to a geo-dispersed environment (one to many).
13	Shall provide edge to core replication. Many to one replication.
14	Shall provide Deduplication on the hardware appliance, not as a software only solution.
15	Shall provide a fully redundant solution and support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
16	Shall provide fast instant restore of files and fast restore of a complete file system to primary storage and to tape without the need to rehydrate and reconstitute data on external or additional disk storage.
17	Shall integrate with _____ Enterprise backup software (to be specified at the delivery order level).
18	Shall provide the ability to be directly attached as a NAS device for a large block sequential I/O data stream.
19	Shall meet the requirement to have a portion of the storage for saving non-deduped data and another portion for deduped data.
20	Shall meet the requirement to select a portion of storage for data replication.
21	Shall provide a built-in capability of self healing that provides corruption recovery during replication.
22	Shall integrate with backup software to backup data directly to tape from the Deduplication secondary storage device.

23	Shall Support a minimum of four nines storage subsystem uptime (or 99.99% availability, excluding planned downtime). (Note: Four Nines (99.99%) = 53 minutes of downtime on a rolling 12 month basis).
24	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
25	Solution shall be able to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
26	Shall provide disk based data Deduplication.
27	Shall provide built-in capability of perform automatic data Integrity checking after data Deduplication.
28	Shall provide secure data Deduplication algorithms.
29	Shall provide built-in capability for self healing that provides corruption recovery when data corruption is detected after Deduplication, without Re-Deduplication of the original data again.
30	Shall provide the ability to rebuild file system from stored metadata.
31	Shall provide the ability to ingest data from multiple sources (from software and/or hardware) simultaneously.
32	Shall provide cover to power switches to prevent inadvertent activation.
33	Shall provide the support of role-based security for access and management of storage devices.
34	Shall support authenticable access with logging (for audits).
35	Shall support a native Management tool able to manage multiple Deduplication Storage devices of the same type in data center implementations.
36	Shall provide a single sign-on integrated with Microsoft Active Directory (AD) or LDAP to manage Deduplication Storage device(s) in a data center implementation from a single master Management console.

37	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
38	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and similar components.
39	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

IP Based Deduplication Storage (Large)	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall provide the minimum usable native disk capacity without data compression, without data Deduplication, and without single instance (no duplicate objects) of 100TB (Terabytes), expandable to a maximum of 500TB (Terabytes).
2	Shall provide a minimum ingest aggregate throughput of 4TB/hr.
3	Solution shall support interoperability between different sized units (Extra large, Large, Medium, and Small)
4	Shall support concurrent parallel I/O streaming.
5	Solution shall provide the ability to support an IP based storage device that supports both Network File System (NFS) v3 or Higher, and Common Internet File System (CIFS) connectivity protocols. All connecting protocols shall support up to the maximum usable storage capacity of the device.
6	Solution shall provide a minimum of two 1GbE and Ethernet ports per system.
7	Solution shall provide a minimum of two 10GbE Ethernet ports per system.
8	Shall provide the support of Jumbo frame, LACP (802.3ad) protocol, and bandwidth aggregation.
9	Shall support Ethernet port expansion to meet storage performance requirements in the same unit(s) as listed above (to be specified at delivery order level) for each storage size types. Capable of adding minimum of two additional ports per system.

10	Solution shall provide storage capacity expansion or scalability with no downtime, no forklift upgrade, no reconfiguration of the internal operating system or re-creation of the existing subsystem components, and remapping connections of the storage subsystem to connecting hosts. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
11	Shall support expansion and scalability of the Data Deduplication System without requiring a forklift upgrade.
12	Shall support that Data residing on the Deduplication device that meets the requirement to replicate to a geo-dispersed environment (one to many).
13	Shall provide edge to core replication. Many to one replication.
14	Shall provide Deduplication on the hardware appliance, not as a software only solution.
15	Shall provide a fully redundant solution and support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
16	Shall provide fast instant restore of files and fast restore of a complete file system to primary storage and to tape without the need to rehydrate and reconstitute data on external or additional disk storage.
17	Shall integrate with _____ Enterprise backup software (to be specified at the delivery order level).
18	Shall provide the ability to be directly attached as a NAS device for a large block sequential I/O data stream.
19	Shall meet the requirement to have a portion of the storage for saving non-deduped data and another portion for deduped data.
20	Shall meet the requirement to select a portion of storage for data replication.
21	Shall provide a built-in capability of self healing that provides corruption recovery during replication.
22	Shall integrate with backup software to backup data directly to tape from the Deduplication secondary storage device.

23	Shall Support a minimum of four nines storage subsystem uptime (or 99.99% availability, excluding planned downtime). (Note: Four Nines (99.99%) = 53 minutes of downtime on a rolling 12 month basis).
24	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
25	Solution shall be able to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
26	Shall provide disk based data Deduplication.
27	Shall provide built-in capability of perform automatic data Integrity checking after data Deduplication.
28	Shall provide secure data Deduplication algorithms.
29	Shall provide built-in capability for self healing that provides corruption recovery when data corruption is detected after Deduplication, without Re-Deduplication of the original data again.
30	Shall provide the ability to rebuild file system from stored metadata.
31	Shall provide the ability to ingest data from multiple sources (from software and/or hardware) simultaneously.
32	Shall provide cover to power switches to prevent inadvertent activation.
33	Shall provide the support of role-based security for access and management of storage devices.
34	Shall support authenticable access with logging (for audits).
35	Shall support a native Management tool able to manage multiple Deduplication Storage devices of the same type in data center implementations.
36	Shall provide a single sign-on integrated with Microsoft Active Directory (AD) or LDAP to manage Deduplication Storage device(s) in a data center implementation from a single master Management console.

37	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
38	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and similar components.
39	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

IP Based Deduplication Storage (Extra Large)	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall provide the minimum usable native disk capacity without data compression, without data Deduplication, and without single instance (no duplicate objects) of 500TB (Terabytes), expandable to at least 750TB (Terabytes).
2	Shall provide a minimum ingest aggregate throughput of 20TB/hr.
3	Solution shall support interoperability between different sized units (Extra large, Large, Medium, and Small)
4	Shall support concurrent parallel I/O streaming.
5	Solution shall provide the ability to support an IP based storage device that supports both Network File System (NFS v3 or Higher, and Common Internet File System (CIFS) connectivity protocols. All connecting protocols shall support up to the maximum usable storage capacity of the device.
6	Solution shall provide a minimum of two 1GbE and Ethernet ports per system.
7	Solution shall provide a minimum of two 10GbE Ethernet ports per system.
8	Shall provide the support of Jumbo frame, LACP (802.3ad) protocol, and bandwidth aggregation.
9	Shall support Ethernet port expansion to meet storage performance requirements in the same unit(s) as listed above (to be specified at delivery order level) for each storage size types. Capable of adding minimum of two additional ports per system.

10	Solution shall provide storage capacity expansion or scalability with no downtime, no forklift upgrade, no reconfiguration of the internal operating system or re-creation of the existing subsystem components, and remapping connections of the storage subsystem to connecting hosts. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
11	Shall support expansion and scalability of the Data Deduplication System without requiring a forklift upgrade.
12	Shall support that Data residing on the Deduplication device that meets the requirement to replicate to a geo-dispersed environment (one to many).
13	Shall provide edge to core replication. Many to one replication.
14	Shall provide Deduplication on the hardware appliance, not as a software only solution.
15	Shall provide a fully redundant solution and support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
16	Shall provide fast instant restore of files and fast restore of a complete file system to primary storage and to tape without the need to rehydrate and reconstitute data on external or additional disk storage.
17	Shall integrate with _____ Enterprise backup software (to be specified at the delivery order level).
18	Shall provide the ability to be directly attached as a NAS device for a large block sequential I/O data stream.
19	Shall meet the requirement to have a portion of the storage for saving non-deduped data and another portion for deduped data.
20	Shall meet the requirement to select a portion of storage for data replication.
21	Shall provide a built-in capability of self healing that provides corruption recovery during replication.
22	Shall integrate with backup software to backup data directly to tape from the Deduplication secondary storage device.

23	Shall Support a minimum of four nines storage subsystem uptime (or 99.99% availability, excluding planned downtime). (Note: Four Nines (99.99%) = 53 minutes of downtime on a rolling 12 month basis).
24	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
25	Solution shall be able to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
26	Shall provide disk based data Deduplication.
27	Shall provide built-in capability of perform automatic data Integrity checking after data Deduplication.
28	Shall provide secure data Deduplication algorithms.
29	Shall provide built-in capability for self healing that provides corruption recovery when data corruption is detected after Deduplication, without Re-Deduplication of the original data again.
30	Shall provide the ability to rebuild file system from stored metadata.
31	Shall provide the ability to ingest data from multiple sources (from software and/or hardware) simultaneously.
32	Shall provide cover to power switches to prevent inadvertent activation.
33	Shall provide the support of role-based security for access and management of storage devices.
34	Shall support authenticable access with logging (for audits).
35	Shall support a native Management tool able to manage multiple Deduplication Storage devices of the same type in data center implementations.
36	Shall provide a single sign-on integrated with Microsoft Active Directory (AD) or LDAP to manage Deduplication Storage device(s) in a data center implementation from a single master Management console.

37	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
38	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and similar components.
39	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

VTL (Virtual Tape Library) with Data Deduplication Storage (Small)	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall provide the minimum usable disk capacity of up to 10TB (Terabytes), expandable to a maximum of 50TB (Terabytes).
2	Shall provide a minimum ingest aggregate throughput of 2TB/hr.
3	Solution shall support a minimum of two (2) 8-Gbit/s or higher Fibre Channel ports per device. All Fibre Channel ports shall be capable of autosensing slower speeds.
4	Solution shall meet the capability of supporting a minimum of two (2) 1GbE Ethernet ports per device.
5	Shall provide support for a minimum of 6 emulated tape libraries.
6	Shall provide support for a minimum of 16 tape drives.
7	Shall provide support for a minimum of 4096 virtual tape cartridges.
8	Solution shall support interoperability between different sized units (Extra large, Large, Medium, and Small)
9	Shall support concurrent parallel I/O streaming.
10	Solution shall provide support for proactively monitoring disk drives and detecting potential failures prior to the failure occurring and taking preventive actions.
11	Solution shall provide Deduplication function and services that integrate with existing backup environment.
12	Shall provide the disk failure redundancy to meet the above ingest throughput requirements.
13	Solution shall support file level restore.
14	Solution shall not require the application to be "off-line" to complete backup activities.
15	Solution shall support compression of backup data.

16	Solution shall provide as backup targets for backup sources such as storage area networks, direct attached storage, network attached storage, and massive array of independent disks.
17	Shall provide fast instant restore of files and fast restore of a complete file system to primary storage and to tape without the need to rehydrate and reconstitute data on external or additional disk storage.
18	Solution shall support ingesting multiple backup job streams to multiple disk targets.
19	Solution shall provide the ability to rebuild file system from stored Metadata.
20	Shall provide a fully redundant solution and support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
21	Shall Support a minimum of four nines storage subsystem uptime (or 99.99% availability, excluding planned downtime). (Note: Four Nines (99.99%) = 53 minutes of downtime on a rolling 12 month basis).
22	Solution shall provide the ability to support minimum of either Fibre Channel (FC) or Internet Small Computer System Interface (iSCSI) connectivity on a single device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
23	Shall provide the ability to support Fibre Channel port expansion to meet the performance requirements as listed above (to be specified at delivery order level) in the same unit(s). Capable of adding additional ports per device.
24	Solution shall meet support of Ethernet port expansion to meet the performance requirements as listed above (to be specified at delivery order level) in the same unit(s). Capable of adding additional ports per device.
25	Solution shall support virtual tape cartridges asynchronous replication.
26	Solution shall support virtual tape libraries asynchronous replication.
27	Shall provide edge to core replication. Many to one replication.

28	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
29	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
30	Solution shall provide cover to power switches to prevent inadvertent activation.
31	Solution shall provide the support of role-based security for access and management of the VTL storage.
32	Shall support authenticable access with logging (for audits).
33	Solution shall support an IP based single master VTL Storage Management Tool able to manage multiple VTL Storage devices of the same type in data center implementations.
34	Solution shall provide a single sign-on integrated with Microsoft Active Directory (AD) or LDAP to manage VTL storage device(s) in a data center implementation from a single master management console.
35	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
36	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and similar components.
37	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

VTL (Virtual Tape Library) with Data Deduplication Storage (Medium)	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall provide the minimum usable disk capacity of 50TB (Terabytes), expandable to a maximum of 100TB (Terabytes).
2	Shall provide a minimum ingest aggregate throughput of 4TB/hr.
3	Solution shall support a minimum of two (2) 8-Gbit/s or higher Fibre Channel ports per device. All Fibre Channel ports shall be capable of autosensing slower speeds.
4	Solution shall meet the capability of supporting a minimum of two (2) 1GbE Ethernet ports per device.
5	Shall provide support for a minimum of 6 emulated tape libraries.
6	Shall provide support for a minimum of 16 tape drives.
7	Shall provide support for a minimum of 4096 virtual tape cartridges.
8	Solution shall support interoperability between different sized units (Extra large, Large, Medium, and Small)
9	Shall support concurrent parallel I/O streaming.
10	Solution shall provide support for proactively monitoring disk drives and detecting potential failures prior to the failure occurring and taking preventive actions.
11	Solution shall provide Deduplication function and services that integrate with existing backup environment.
12	Shall provide the disk failure redundancy to meet the above ingest throughput requirements.
13	Solution shall support file level restore.
14	Solution shall not require the application to be "off-line" to complete backup activities.
15	Solution shall support compression of backup data.

16	Solution shall provide as backup targets for backup sources such as storage area networks, direct attached storage, network attached storage, and massive array of independent disks.
17	Shall provide fast instant restore of files and fast restore of a complete file system to primary storage and to tape without the need to rehydrate and reconstitute data on external or additional disk storage.
18	Solution shall support ingesting multiple backup job streams to multiple disk targets.
19	Solution shall provide the ability to rebuild file system from stored Metadata.
20	Shall provide a fully redundant solution and support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
21	Shall Support a minimum of four nines storage subsystem uptime (or 99.99% availability, excluding planned downtime). (Note: Four Nines (99.99%) = 53 minutes of downtime on a rolling 12 month basis).
22	Solution shall provide the ability to support minimum of either Fibre Channel (FC) or Internet Small Computer System Interface (iSCSI) connectivity on a single device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
23	Shall provide the ability to support Fibre Channel port expansion to meet the performance requirements as listed above (to be specified at delivery order level) in the same unit(s). Capable of adding additional ports per device.
24	Solution shall meet support of Ethernet port expansion to meet the performance requirements as listed above (to be specified at delivery order level) in the same unit(s). Capable of adding additional ports per device.
25	Solution shall support virtual tape cartridges asynchronous replication.
26	Solution shall support virtual tape libraries asynchronous replication.
27	Shall provide edge to core replication. Many to one replication.

28	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
29	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
30	Solution shall provide cover to power switches to prevent inadvertent activation.
31	Solution shall provide the support of role-based security for access and management of the VTL storage.
32	Shall support authenticable access with logging (for audits).
33	Solution shall support an IP based single master VTL Storage Management Tool able to manage multiple VTL Storage devices of the same type in data center implementations.
34	Solution shall provide a single sign-on integrated with Microsoft Active Directory (AD) or LDAP to manage VTL storage device(s) in a data center implementation from a single master management console.
35	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
36	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and similar components.
37	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

VTL (Virtual Tape Library) with Data Deduplication Storage (Large)	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall provide the minimum usable disk capacity of 100TB (Terabytes), expandable to a maximum of 500TB (Terabytes).
2	Shall provide a minimum ingest aggregate throughput of 6TB/hr.
3	Solution shall support a minimum of four (4) 8-Gbit/s or higher Fibre Channel ports per device. All Fibre Channel ports shall be capable of autosensing slower speeds.
4	Solution shall meet the capability of supporting a minimum of four (4) 1GbE Ethernet ports per device.
5	Shall provide support for a minimum of 12 emulated tape libraries.
6	Shall provide support for a minimum of 32 tape drives.
7	Shall provide support for a minimum of 8192 virtual tape cartridges.
8	Solution shall support interoperability between different sized units (Extra large, Large, Medium, and Small)
9	Shall support concurrent parallel I/O streaming.
10	Solution shall provide support for proactively monitoring disk drives and detecting potential failures prior to the failure occurring and taking preventive actions.
11	Solution shall provide Deduplication function and services that integrate with existing backup environment.
12	Shall provide the disk failure redundancy to meet the above ingest throughput requirements.
13	Solution shall support file level restore.
14	Solution shall not require the application to be "off-line" to complete backup activities.
15	Solution shall support compression of backup data.

16	Solution shall provide as backup targets for backup sources such as storage area networks, direct attached storage, network attached storage, and massive array of independent disks.
17	Shall provide fast instant restore of files and fast restore of a complete file system to primary storage and to tape without the need to rehydrate and reconstitute data on external or additional disk storage.
18	Solution shall support ingesting multiple backup job streams to multiple disk targets.
19	Solution shall provide the ability to rebuild file system from stored Metadata.
20	Shall provide a fully redundant solution and support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
21	Shall Support a minimum of four nines storage subsystem uptime (or 99.99% availability, excluding planned downtime). (Note: Four Nines (99.99%) = 53 minutes of downtime on a rolling 12 month basis).
22	Solution shall provide the ability to support minimum of either Fibre Channel (FC) or Internet Small Computer System Interface (iSCSI) connectivity on a single device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
23	Shall provide the ability to support Fibre Channel port expansion to meet the performance requirements as listed above (to be specified at delivery order level) in the same unit(s). Capable of adding additional ports per device.
24	Solution shall meet support of Ethernet port expansion to meet the performance requirements as listed above (to be specified at delivery order level) in the same unit(s). Capable of adding additional ports per device.
25	Solution shall support virtual tape cartridges asynchronous replication.
26	Solution shall support virtual tape libraries asynchronous replication.
27	Shall provide edge to core replication. Many to one replication.

28	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
29	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
30	Solution shall provide cover to power switches to prevent inadvertent activation.
31	Solution shall provide the support of role-based security for access and management of the VTL storage.
32	Shall support authenticable access with logging (for audits).
33	Solution shall support an IP based single master VTL Storage Management Tool able to manage multiple VTL Storage devices of the same type in data center implementations.
34	Solution shall provide a single sign-on integrated with Microsoft Active Directory (AD) or LDAP to manage VTL storage device(s) in a data center implementation from a single master management console.
35	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
36	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and similar components.
37	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

VTL (Virtual Tape Library) with Data Deduplication Storage (Extra Large)	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall provide the minimum usable disk capacity of 500TB (Terabytes), expandable to at least 750TB (Terabytes).
2	Shall provide a minimum ingest aggregate throughput of 8TB/hr.
3	Solution shall support a minimum of four (4) 8-Gbit/s or higher Fibre Channel ports per device. All Fibre Channel ports shall be capable of autosensing slower speeds.
4	Solution shall meet the capability of supporting a minimum of four (4) 1GbE Ethernet ports per device.
5	Shall provide support for a minimum of 12 emulated tape libraries.
6	Shall provide support for a minimum of 32 tape drives.
7	Shall provide support for a minimum of 8192 virtual tape cartridges.
8	Solution shall support interoperability between different sized units (Extra large, Large, Medium, and Small)
9	Shall support concurrent parallel I/O streaming.
10	Solution shall provide support for proactively monitoring disk drives and detecting potential failures prior to the failure occurring and taking preventive actions.
11	Solution shall provide Deduplication function and services that integrate with existing backup environment.
12	Shall provide the disk failure redundancy to meet the above ingest throughput requirements.
13	Solution shall support file level restore.
14	Solution shall not require the application to be "off-line" to complete backup activities.
15	Solution shall support compression of backup data.

16	Solution shall provide as backup targets for backup sources such as storage area networks, direct attached storage, network attached storage, and massive array of independent disks.
17	Shall provide fast instant restore of files and fast restore of a complete file system to primary storage and to tape without the need to rehydrate and reconstitute data on external or additional disk storage.
18	Solution shall support ingesting multiple backup job streams to multiple disk targets.
19	Solution shall provide the ability to rebuild file system from stored Metadata.
20	Shall provide a fully redundant solution and support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
21	Shall Support a minimum of four nines storage subsystem uptime (or 99.99% availability, excluding planned downtime). (Note: Four Nines (99.99%) = 53 minutes of downtime on a rolling 12 month basis).
22	Solution shall provide the ability to support minimum of either Fibre Channel (FC) or Internet Small Computer System Interface (iSCSI) connectivity on a single device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
23	Shall provide the ability to support Fibre Channel port expansion to meet the performance requirements as listed above (to be specified at delivery order level) in the same unit(s). Capable of adding additional ports per device.
24	Solution shall meet support of Ethernet port expansion to meet the performance requirements as listed above (to be specified at delivery order level) in the same unit(s). Capable of adding additional ports per device.
25	Solution shall support virtual tape cartridges asynchronous replication.
26	Solution shall support virtual tape libraries asynchronous replication.
27	Shall provide edge to core replication. Many to one replication.

28	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
29	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
30	Solution shall provide cover to power switches to prevent inadvertent activation.
31	Solution shall provide the support of role-based security for access and management of the VTL storage.
32	Shall support authenticable access with logging (for audits).
33	Solution shall support an IP based single master VTL Storage Management Tool able to manage multiple VTL Storage devices of the same type in data center implementations.
34	Solution shall provide a single sign-on integrated with Microsoft Active Directory (AD) or LDAP to manage VTL storage device(s) in a data center implementation from a single master management console.
35	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
36	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and similar components.
37	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

Low Performance Unified Storage	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support a minimum of 20,000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
2	Shall support minimum of 1000 MBytes per second throughput.
3	Shall provide the minimum usable disk capacity of 25 TB . This initial data storage capacity must be distributed evenly among two or more shelves in order for future local mirroring between shelves.
4	Shall be capable of supporting a minimum of two (2) 8-Gbit/s Fibre Channel ports per controller. All Fibre Channel ports shall be capable of autosensing slower speeds of 2 & 4 Gbit/s.
5	Shall be capable of supporting a minimum of two (2) 1GbE Ethernet or iSCSI ports per controller.
6	Shall be capable of supporting a minimum of one (1) 10GbE iSCSI or Ethernet ports per controller.
7	Shall provide, excluding space on Storage System Operating System (OS) Drives, the initial data storage capacity must be distributed evenly among multiple shelves and support mirroring between shelves.
8	Shall provide the disk failure redundancy configuration to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
9	Shall provide the appropriate disk drive technologies to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
10	Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.

11	Shall provide capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
12	Shall Support a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
13	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
14	Shall provide a minimum of two storage controllers in a module for controller based storage solution, which are load balanced and provide automatic failover including the ability to maintain access to all data through a controller failure.
15	Shall provide the ability to upgrade a controller on the storage system without replacing the storage subsystem. The upgrade of the controller shall be non-destructive to the data, requiring no data migration, no reconfiguration and no LUN remapping to any connecting Host.
16	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
17	Shall support adding, upgrading or replacing storage subsystem components while adhering to the required storage device uptime requirement, redundancy and needing no data migration.
18	Shall provide the ability to expand and scale Host side connectivity and backend capacity independently in order to increase performance.
19	Shall provide storage subsystem support boot from SAN.
20	Shall support a changeable LUN UDID value.

21	Shall support the ability to create LUNs and Volumes across multiple spindles.
22	Shall support dynamic LUN and Volume expansion.
23	Shall be able to present a minimum of 15TB volume to connecting hosts.
24	Shall provide the ability to use “Thin Provisioning” or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
25	Shall provide that storage subsystem performance will not be affected when using “Thin Provisioning”.
26	Shall provide the capability of supporting Fibre Channel (FC), Internet Small Computer System Interface (iSCSI), Network File System V4 (NFS), and Common Internet File System (CIFS) connectivity simultaneously on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
27	Shall support the ability to expand Fibre Channel ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
28	Shall be capable of supporting Jumbo frame and LACP protocol.
29	Shall support the ability to expand iSCSI ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
30	Shall be capable of supporting native 10GbE Fibre Channel over Ethernet (FCoE) host connections.
31	Shall be capable of supporting 10GbE Ethernet ports.
32	Solution shall support a minimum of 256 SCSI initiators (host connections).
33	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
34	Shall provide the capability of synchronous and asynchronous replication with write order fidelity.
35	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.

36	Solution shall be able to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
37	Shall be able to allow source update during data migration. Online data migration from other storage devices and data migration is transparent to users.
38	Shall be capable of maintaining redundancy and the performance metrics requirements as stated above during snapshot and clone operations.
39	Power Switches shall be covered to prevent inadvertent activation.
40	Shall support role-based security or audit trail logging for access to storage.
41	Shall provide a single master management interface to manage multiple storage subsystems of the same type in data center implementations.
42	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
43	Shall have a graphical user interface (GUI) or command (CLI), or a Wizard to automate the process to provision a large number of Disk Groups, Volumes and LUNs.
44	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.
45	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.
46	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

Medium Performance Unified Storage	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support a minimum of 50,000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
2	Shall support minimum of 2500 MBytes per second throughput.
3	Shall provide the minimum usable disk capacity of 50 TB . This initial data storage capacity must be distributed evenly among two or more shelves in order for future local mirroring between shelves.
4	Shall be capable of supporting a minimum of four (4) 8-Gbit/s Fibre Channel ports per controller. All Fibre Channel ports shall be capable of autosensing slower speeds of 2 & 4 Gbit/s.
5	Shall be capable of supporting a minimum of four (4) 1GbE Ethernet or iSCSI ports per controller.
6	Shall be capable of supporting a minimum of two (2) 10GbE iSCSI or Ethernet ports per controller.
7	Shall provide, excluding space on Storage System Operating System (OS) Drives, the initial data storage capacity must be distributed evenly among multiple shelves and support mirroring between shelves.
8	Shall provide the disk failure redundancy configuration to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
9	Shall provide the appropriate disk drive technologies to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
10	Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.

11	Shall provide capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
12	Shall Support a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
13	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
14	Shall provide a minimum of two storage controllers in a module for controller based storage solution, which are load balanced and provide automatic failover including the ability to maintain access to all data through a controller failure.
15	Shall provide the ability to upgrade a controller on the storage system without replacing the storage subsystem. The upgrade of the controller shall be non-destructive to the data, requiring no data migration, no reconfiguration and no LUN remapping to any connecting Host.
16	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
17	Shall support adding, upgrading or replacing storage subsystem components while adhering to the required storage device uptime requirement, redundancy and needing no data migration.
18	Shall provide the ability to expand and scale Host side connectivity and backend capacity independently in order to increase performance.
19	Shall provide storage subsystem support boot from SAN.
20	Shall support a changeable LUN UDID value.

21	Shall support the ability to create LUNs and Volumes across multiple spindles.
22	Shall support dynamic LUN and Volume expansion.
23	Shall be able to present a minimum of 15TB volume to connecting hosts.
24	Shall provide the ability to use “Thin Provisioning” or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
25	Shall provide that storage subsystem performance will not be affected when using “Thin Provisioning”.
26	Shall provide the capability of supporting Fibre Channel (FC), Internet Small Computer System Interface (iSCSI), Network File System V4 (NFS), and Common Internet File System (CIFS) connectivity simultaneously on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
27	Shall support the ability to expand Fibre Channel ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
28	Shall be capable of supporting Jumbo frame and LACP protocol.
29	Shall support the ability to expand iSCSI ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
30	Shall be capable of supporting native 10GbE Fibre Channel over Ethernet (FCoE) host connections.
31	Shall be capable of supporting 10GbE Ethernet ports.
32	Solution shall support a minimum of 256 SCSI initiators (host connections).
33	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
34	Shall provide the capability of synchronous and asynchronous replication with write order fidelity.
35	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.

36	Solution shall be able to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
37	Shall be able to allow source update during data migration. Online data migration from other storage devices and data migration is transparent to users.
38	Shall be capable of maintaining redundancy and the performance metrics requirements as stated above during snapshot and clone operations.
39	Power Switches shall be covered to prevent inadvertent activation.
40	Shall support role-based security or audit trail logging for access to storage.
41	Shall provide a single master management interface to manage multiple storage subsystems of the same type in data center implementations.
42	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
43	Shall have a graphical user interface (GUI) or command (CLI), or a Wizard to automate the process to provision a large number of Disk Groups, Volumes and LUNs.
44	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.
45	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.
46	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

High Performance Unified Storage	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall support a minimum of 100,000 I/Os per second during all system functions including snapshot and clone operations. Solution shall utilize appropriate disk type, spindle count, and raid type to meet I/O requirements.
2	Shall support minimum of 5000 MBytes per second throughput.
3	Shall provide the minimum usable disk capacity of 75 TB . This initial data storage capacity must be distributed evenly among two or more shelves in order for future local mirroring between shelves.
4	Shall be capable of supporting a minimum of four (4) 8-Gbit/s Fibre Channel ports per controller. All Fibre Channel ports shall be capable of autosensing slower speeds of 2 & 4 Gbit/s.
5	Shall be capable of supporting a minimum of four (4) 1GbE Ethernet or iSCSI ports per controller.
6	Shall be capable of supporting a minimum of two (2) 10GbE iSCSI or Ethernet ports per controller.
7	Shall provide, excluding space on Storage System Operating System (OS) Drives, the initial data storage capacity must be distributed evenly among multiple shelves and support mirroring between shelves.
8	Shall provide the disk failure redundancy configuration to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
9	Shall provide the appropriate disk drive technologies to meet the above capacity, IOPs and workload performance requirements (to be specified at delivery order level).
10	Shall provide capability of creating a minimum of 200 space efficient pointer based point in time copies per Storage System.

11	Shall provide capability of creating point in time delta clone (Delta clone is a copy based on pointers to the original data, which is updated when changes occur to the original data), Clones shall be space efficient on an as needed basis with no space reservation.
12	Shall Support a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
13	Shall provide redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
14	Shall provide a minimum of two storage controllers in a module for controller based storage solution, which are load balanced and provide automatic failover including the ability to maintain access to all data through a controller failure.
15	Shall provide the ability to upgrade a controller on the storage system without replacing the storage subsystem. The upgrade of the controller shall be non-destructive to the data, requiring no data migration, no reconfiguration and no LUN remapping to any connecting Host.
16	Shall provide storage capacity expansion with no reconfiguration or LUN remapping of the storage device. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
17	Shall support adding, upgrading or replacing storage subsystem components while adhering to the required storage device uptime requirement, redundancy and needing no data migration.
18	Shall provide the ability to expand and scale Host side connectivity and backend capacity independently in order to increase performance.
19	Shall provide storage subsystem support boot from SAN.
20	Shall support a changeable LUN UDID value.

21	Shall support the ability to create LUNs and Volumes across multiple spindles.
22	Shall support dynamic LUN and Volume expansion.
23	Shall be able to present a minimum of 15TB volume to connecting hosts.
24	Shall provide the ability to use “Thin Provisioning” or to over provision/over allocate storage capacity to hosts, allowing hosts to view more logical storage capacity than has been physically reserved on the storage array.
25	Shall provide that storage subsystem performance will not be affected when using “Thin Provisioning”.
26	Shall provide the capability of supporting Fibre Channel (FC), Internet Small Computer System Interface (iSCSI), Network File System V4 (NFS), and Common Internet File System (CIFS) connectivity simultaneously on a single storage device. All connecting protocols shall support up to the maximum usable storage capacity of the device.
27	Shall support the ability to expand Fibre Channel ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
28	Shall be capable of supporting Jumbo frame and LACP protocol.
29	Shall support the ability to expand iSCSI ports non-disruptively, when adding additional ports per controller and still maintain storage performance requirements in the same system.
30	Shall be capable of supporting native 10GbE Fibre Channel over Ethernet (FCoE) host connections.
31	Shall be capable of supporting 10GbE Ethernet ports.
32	Solution shall support a minimum of 256 SCSI initiators (host connections).
33	Shall provide load balance multi path failover software and multi mount points when using Ethernet.
34	Shall provide the capability of synchronous and asynchronous replication with write order fidelity.
35	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.

36	Solution shall be able to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
37	Shall be able to allow source update during data migration. Online data migration from other storage devices and data migration is transparent to users.
38	Shall be capable of maintaining redundancy and the performance metrics requirements as stated above during snapshot and clone operations.
39	Power Switches shall be covered to prevent inadvertent activation.
40	Shall support role-based security or audit trail logging for access to storage.
41	Shall provide a single master management interface to manage multiple storage subsystems of the same type in data center implementations.
42	Shall provide a single sign-on integrated with Microsoft Active Directory (AD)/or LDAP to manage storage device(s) in a data center implementation from a single master management console.
43	Shall have a graphical user interface (GUI) or command (CLI), or a Wizard to automate the process to provision a large number of Disk Groups, Volumes and LUNs.
44	Shall have the native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information shall be capable of being transmitted to the Vendor or OEM as defined by the contract and designated VA Point of Contact.
45	Shall have the native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans, Power Supplies and similar components.
46	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

Archive Storage (Small)	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall provide an initial minimum usable disk capacity of 50TB (Terabytes), expandable to a maximum of 100TB (Terabytes).
2	Shall provide intelligent power management system with the ability to enter a disk power reduction mode for inactive data.
3	Shall integrate and present as a target to leading major Enterprise backup software.
4	Shall provide active background data integrity verification.
5	Shall be able to proactively monitor and provide background disk scrubbing to detect potential drive failures and automatically move data to spare drive from a suspected faulty disk drive.
6	Shall Support a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
7	Shall provide a minimum aggregate ingestion throughput rate of 3.2TB/hr per system.
8	Shall provide concurrent parallel I/O streaming.
9	Shall support a dense storage capacity and small storage foot print by providing a minimum of 1PB (Petabyte) of storage in two (2) cabinets or less.
10	Shall support native or host/appliance based write-once-read-many (WORM) operation.
11	Shall support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.

12	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
13	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
14	Shall provide host/appliance based or native Asynchronous replication.
15	Shall support CIFS, NFS V4, and TCP/IP connectivity.
16	Shall provide a minimum of (2) 8Gbit or higher speed fibre ports per system and be capable of autosensing slower speeds.
17	Shall provide a Minimum of (2) 1GbE or higher Ethernet ports per system.
18	Shall provide the ability to support port expansion non-disruptively to meet the storage performance requirements as listed above (to be specified at delivery order level) in the same unit(s).
19	Power Switches shall be covered to prevent inadvertent activation.
20	Shall provide the support of role-based security for access and management of storage devices.
21	Shall support authenticable access with logging (for audits).
22	Shall provide a single master management interface to manage multiple storage devices of the same type in data center implementations.
23	Shall provide a single sign-on integrated with Microsoft Active Directory (AD) or LDAP to manage storage device(s) in a data center implementation from a single master management console.
24	Shall have a graphical user interface (GUI) or command line interface (CLI) or wizard to automate the process to provision a large number of Disk Groups, Volumes or LUNs.

25	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
26	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and similar components.
27	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

Archive Storage (Medium)	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall provide minimum usable disk capacity of 500TB (Terabytes), expandable to a maximum of 1PB (Petabyte).
2	Shall provide intelligent power management system with the ability to enter a disk power reduction mode for inactive data.
3	Shall integrate and present as a target to leading major Enterprise backup software.
4	Shall provide active background data integrity verification.
5	Shall be able to proactively monitor and provide background disk scrubbing to detect potential drive failures and automatically move data to spare drive from a suspected faulty disk drive.
6	Shall Support a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
7	Shall provide a minimum aggregate ingestion throughput rate of 5.2TB/hr per system.
8	Shall provide concurrent parallel I/O streaming.
9	Shall support a dense storage capacity and small storage foot print by providing a minimum of 1PB (Petabyte) of storage in two (2) cabinets or less.
10	Shall support native or host/appliance based write-once-read-many (WORM) operation.
11	Shall support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.

12	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
13	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
14	Shall provide host/appliance based or native Asynchronous replication.
15	Shall support CIFS, NFS V4, and TCP/IP connectivity.
16	Shall provide a minimum of (2) 8Gbit or higher speed fibre ports per system and be capable of autosensing slower speeds.
17	Shall provide a Minimum of (2) 1GbE or higher Ethernet ports per system.
18	Shall provide the ability to support port expansion non-disruptively to meet the storage performance requirements as listed above (to be specified at delivery order level) in the same unit(s).
19	Power Switches shall be covered to prevent inadvertent activation.
20	Shall provide the support of role-based security for access and management of storage devices.
21	Shall support authenticable access with logging (for audits).
22	Shall provide a single master management interface to manage multiple storage devices of the same type in data center implementations.
23	Shall provide a single sign-on integrated with Microsoft Active Directory (AD) or LDAP to manage storage device(s) in a data center implementation from a single master management console.
24	Shall have a graphical user interface (GUI) or command line interface (CLI) or wizard to automate the process to provision a large number of Disk Groups, Volumes or LUNs.

25	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
26	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and similar components.
27	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

Archive Storage (Large)	
OEM Model/Part Number:	
Reference Number	Requirements
1	Shall provide minimum usable disk capacity of at least 1PB (Petabyte).
2	Shall provide intelligent power management system with the ability to enter a disk power reduction mode for inactive data.
3	Shall integrate and present as a target to leading major Enterprise backup software.
4	Shall provide active background data integrity verification.
5	Shall be able to proactively monitor and provide background disk scrubbing to detect potential drive failures and automatically move data to spare drive from a suspected faulty disk drive.
6	Shall Support a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis).
7	Shall provide a minimum aggregate ingestion throughput rate of 5.2TB/hr per system.
8	Shall provide concurrent parallel I/O streaming.
9	Shall support a dense storage capacity and small storage foot print by providing a minimum of 1PB (Petabyte) of storage in two (2) cabinets or less.
10	Shall support native or host/appliance based write-once-read-many (WORM) operation.
11	Shall support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.

12	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
13	Solution shall provide the ability to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
14	Shall provide host/appliance based or native Asynchronous replication.
15	Shall support CIFS, NFS V4, and TCP/IP connectivity.
16	Shall provide a minimum of (2) 8Gbit or higher speed fibre ports per system and be capable of autosensing slower speeds.
17	Shall provide a Minimum of (2) 1GbE or higher Ethernet ports per system.
18	Shall provide the ability to support port expansion non-disruptively to meet the storage performance requirements as listed above (to be specified at delivery order level) in the same unit(s).
19	Power Switches shall be covered to prevent inadvertent activation.
20	Shall provide the support of role-based security for access and management of storage devices.
21	Shall support authenticable access with logging (for audits).
22	Shall provide a single master management interface to manage multiple storage devices of the same type in data center implementations.
23	Shall provide a single sign-on integrated with Microsoft Active Directory (AD) or LDAP to manage storage device(s) in a data center implementation from a single master management console.
24	Shall have a graphical user interface (GUI) or command line interface (CLI) or wizard to automate the process to provision a large number of Disk Groups, Volumes or LUNs.

25	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact.
26	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and similar components.
27	Shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process.

	GRID Based Object Storage (Small)
	OEM Model/Part Number:
Reference Number	Requirements
1	Solution shall provide minimum usable native disk capacity without data compression, without data deduplication, and without single instance (no duplicate objects) of 20TB (Terabytes), expandable to a maximum of 50TB (Terabytes).
2	Solution shall provide a minimum of Enterprise grade SATA spinning disks or better as the backend storage devices to store the object data.
3	The solution shall not include removable media, such as optical, tapes and removable disk cartridge.
4	Solution shall support minimum of Representational State Transfer (REST), Common Internet File System (CIFS), and Network File System (NFS) protocol.

5	Solution shall provide an intelligent policy-based object storage system. Solution shall be fully automated, policy driven without manual intervention, script, or wizard based automation to manage data retention, replication, and data distribution policies. For example, if the policy is defined to have 1 copy of the data locally at the primary site and 1 copy of the data at the remote site. In the event when primary site is not able to communicate with the remote site due to a temporary outage at the remote site, the solution shall automatically create a temporary remote copy at a remote tertiary site intelligently or a user defined temporary remote tertiary location during the creation of the policy process to meet the policy requirement (1 local and 1 remote). When the communication to the original remote site is restored, the solution will update and re-synchronize the missing data automatically to the original remote site and automatically delete the temporary remote copy at the temporary remote tertiary location. The solution shall automatically perform self healing of the system during a non-disaster type of outage. An alert and logging mechanism shall be included in the solution to capture the sequence of activities and provide the final status via email to the designated recipient(s).
6	Solution shall provide customizable policy to define the number of synchronous local data copies, the number of asynchronous remote data copies, the number of sites to store the data, the primary site location, the disaster recover (DR) site location and the temporary remote tertiary site location.
7	The solution shall have the ability to provide automatic or user definable thresholds in the policy to determine temporary interruptions (such as system resource and/or communication problems) when accessing the DR site. This capability is used to determine when the remote copy of the data shall be copied to the temporary tertiary site.

8	The Contractor shall provide a single Graphic User Interface (GUI) that allows more than one creations, editions, and deletions of data retention, replication, and data distribution policies in a one single process. For example, data retention, replication, and data distribution policies can be configured in one GUI interface and not to have separate individual interfaces for data retention, replication, and data distribution respectively.
9	Solution shall replicate files to the remote site based on available WAN bandwidth and remote system resources. The process shall be fully automated, policy driven without manual intervention, script or wizard based automation.
10	Solution shall provide the necessary equipments at the secondary remote site so that the remote site can be promoted to primary site role in the event of total disaster at the primary site.
11	In the event of a site recovery, the solution shall be capable of creating a duplicate system by copying all data from the Disaster Recovery site which will be shipped to the disaster site to be recovered.
12	Solution shall provide storage capacity expansion or scalability with no downtime, no forklift upgrade, no reconfiguration of the internal operating system, and LUN remapping of the storage subsystem to connecting hosts. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
13	Solution shall support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
14	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.

15	Solution shall be able to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
16	Solution shall provide File Transfer ingest rate to local storage solution at a minimum of 1.5 Gigabytes (GB) of data per minute (1.5GB/min).
17	Shall Support a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis)
18	Solution shall always maintain original file attributes (Create, Access dates, file permission, and security or other attributes) for all data replication process, data copy process including data restoration processes. The file attributes are to stay with the file.
19	Solution shall provide the ability to verify data after it has been transferred from the local site to the remote location to ensure it matches with no data corruption. If verification of data fails solution shall resend the data. The copy of file at the remote site shall be identical to the copy of the image file at the local site after replication. This check shall be performed automatically.
20	Solution shall automatically (based on policy, not manual, script or wizard based) redirect the read processes to remote storage devices/components if the local storage devices/components are not available during image file read process.
21	Solution shall provide a solution that can automatically (based on policy, not manual, script or wizard based) redirect the write processes to remote storage node and/or backend storage if the local storage node and/or backend storage is not available during image file write process.

22	The solution shall present a CIFS interface that is addressable by a Microsoft Active Directory fully qualified path. The Solution shall present a redundant CIFS interface. It must be presented to any windows client on the network. Any windows client on the network must be able to authenticate to the server and access to the share.
23	The Contractor shall provide a redundant Global Namespace object based Archive system. All objects shall be retrievable via web browser (http and https) based on its object metadata definitions.
24	Solution shall maintain mappings of the Common Internet File System (CIFS) share in the event that the primary local gateway is unavailable or offline. The solution shall continue to function automatically with no manual intervention, script or wizard based automation on local secondary gateway with the same CIFS mapping. The path used to access the CIFS shares will be the same regardless of whether the local or remote copy of the image is accessed.
25	Solution shall provide a process automatically (based on policy, not manual, script or wizard based) update and resynchronize the recovered local site archive storage from the remote archive storage when the local archive storage is back online after a period of downtime. The process shall be fully automated, policy driven without manual intervention, script or wizard based automation
26	Solution shall provide a process to log all file transfer success or failure.
27	Solution shall utilize Microsoft Active Directory for all security permissions for the whole system management and data access.
28	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system components problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact

29	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and other similar components.
30	Solution shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process and SMTP mail.
31	Solution shall escalate alerts when storage space utilization falls below a user defined threshold.
32	Solution shall provide a means for the solution to log the file transfer time from local archive to remote site as a user defined threshold. (e.g. If logging transfer time is set to 60 seconds and the actual transfer time exceeds 60 seconds it shall be logged).
33	Solution shall support the function to access remote data from the local archive location for display purposes.
34	Solution shall provide a means for the Solution to retrieve a copy of the data from the remote archive locations for storage at the local archive location if the local archive was not available.
35	Solution shall log file access, create and modify dates for retention statistics and monitoring purposes.
36	Solution shall under normal operating conditions, replicate data immediately. In no case shall the replication backlog be greater than four (4) hours of data.
37	Solution shall be able to scale components such as network interface cards, adapter ports, processors, memory, and storage capacity independently.
38	Solution shall monitor and access the remote data with the least amount of file transfer latency.
39	Solution shall manage, control, and define policies (policy that defines the number of data replication copies, the location, and the temporary remote tertiary site location) in the Object storage device.
40	Solution shall be capable to capture and/or log performance data such as data ingest rate, data ingest size, data replication bandwidth utilization, data replication latency, data retrieval response time and others.
41	Solution shall support a minimum of two 1Gb Ethernet connectivity to the local production LAN.

42	Solution shall provide redundant Power Distribution Unit (PDUs) with sufficient outlets to power all units in the rack(s).																														
43	Solution equipment shall be Pre-installed and Pre-cabled in a 42U Rack prior to delivery. All cables and components installed in the rack shall be labeled.																														
44	Solution shall include Pre-installed and Pre-cabled redundant top of the rack network switches in every rack provided to minimize the number of network connections to VA Core network switches. The top of the rack switches provided in the solution shall be interoperable with existing VA Core network switches.																														
45	Solution shall support Internet Protocol version 6 (IPv6).																														
46	Solution shall support a minimum of the following file formats: <table> <tr> <td>AVI</td><td>Motion Video AVI</td></tr> <tr> <td>BMP</td><td>Bitmap file BMP</td></tr> <tr> <td>DCM</td><td>Dicom file DCM</td></tr> <tr> <td>HTML</td><td>Web Document HTML</td></tr> <tr> <td>JPG</td><td>Full Color JPG</td></tr> <tr> <td>MHTML</td><td>MIME HTML Document</td></tr> <tr> <td>MP3</td><td>Motion Video MPEG-3</td></tr> <tr> <td>MP4</td><td>Motion Video MPEG-4</td></tr> <tr> <td>MPG</td><td>Motion Video MPG</td></tr> <tr> <td>PDF</td><td>Adobe PDF</td></tr> <tr> <td>RTF</td><td>Rich Text format RTF</td></tr> <tr> <td>TGA</td><td>Targa Image TGA</td></tr> <tr> <td>TIF</td><td>Scanned Document TIF</td></tr> <tr> <td>TXT</td><td>Text file import TXT</td></tr> <tr> <td>WAV</td><td>Audio file WAV</td></tr> </table>	AVI	Motion Video AVI	BMP	Bitmap file BMP	DCM	Dicom file DCM	HTML	Web Document HTML	JPG	Full Color JPG	MHTML	MIME HTML Document	MP3	Motion Video MPEG-3	MP4	Motion Video MPEG-4	MPG	Motion Video MPG	PDF	Adobe PDF	RTF	Rich Text format RTF	TGA	Targa Image TGA	TIF	Scanned Document TIF	TXT	Text file import TXT	WAV	Audio file WAV
AVI	Motion Video AVI																														
BMP	Bitmap file BMP																														
DCM	Dicom file DCM																														
HTML	Web Document HTML																														
JPG	Full Color JPG																														
MHTML	MIME HTML Document																														
MP3	Motion Video MPEG-3																														
MP4	Motion Video MPEG-4																														
MPG	Motion Video MPG																														
PDF	Adobe PDF																														
RTF	Rich Text format RTF																														
TGA	Targa Image TGA																														
TIF	Scanned Document TIF																														
TXT	Text file import TXT																														
WAV	Audio file WAV																														
47	Solution shall make the file transfer process transparent to end users with no user intervention needed. The physical location of the data repository shall be transparent to end user.																														
48	Solution shall perform automatic restoration of a corrupted file (Object/File Data and Meta Data) from a Disaster Recovery (DR) copy.																														
49	Solution shall automatically resume or recover from file transfer failures.																														

50	Solution shall provide capability to log events and problems and provide the ability to manually set the level of logging and reporting.
51	Solution shall provide a role based configuration with a minimum of a system user role which allows for a system user to view current hardware status and a Super User system administration role which allows for an administrator to configure system policies, and parameters.
52	Solution shall provide a web based single master management administrative console without the need to install client software for control of system software implementation, policies and user management protected with permission roles.
53	Solution shall utilize Microsoft Active Directory to provide a single sign-on to the management web console and the log on security shall provide the permission to access and manage all the CIFS shares and data.
54	Solution shall log the software version/installed hardware/firmware versions at each site.
55	Solution shall provide interface callable from an application using HTTP/S Web Services using SOAP or REST and Get/Post methods for moving binary data. The ICD/WSDL will be included with the solution.
56	Solution shall provide a web interface to access the metadata of the files/objects that are stored in the storage device.
57	Solution shall provide web interface to access the system logs generated by all components. If separate logs are generated the interface will include the ability to determine what logs are available and parameters to select specific logs.
58	Solution shall provide a web interface to access files by file path/name.
59	Solution shall provide a web interface to store files by file path/name.
60	Solution shall provide Web interface that provides usage statistics (metrics on all nodes –size, amount full, number of files, as examples).
61	Solution shall provide web interface that provides access to the list of files by attributes (MIME type, date created/range, size, file name or partial file name).

62	Solution shall provide a web interface that will export/copy files by attributes (e.g. File path or partial file path) to a specified target CFIS Share.
63	Solution shall provide a web interface that provides file statistics (e.g., size, creation date, modify date, access date) given File name or file path, or File/Object ID specified by the solution.
64	Solution shall provide web interface that provides image retrieval time statistics given an Object/File ID or file path.
65	Solution shall provide a web interface that provides the "Health status" of the storage (i.e. what is the current status of each of the nodes on the network or of a particular node).
66	Solution shall provide a web interface that provides status of devices (e.g. any disk errors or outages.)
67	Solution shall provide web interface that provides the physical location of Storage devices given a device ID supplied by the vendor, or the list of storage devices and characteristics for all devices at a location.

	GRID Based Object Storage (Medium)
	OEM Model/Part Number:
Reference Number	Requirements
1	Solution shall provide minimum usable native disk capacity without data compression, without data deduplication, and without single instance (no duplicate objects) of 50TB (Terabytes), expandable to a maximum of 100TB (Terabytes).
2	Solution shall provide a minimum of Enterprise grade SATA spinning disks or better as the backend storage devices to store the object data.
3	The solution shall not include removable media, such as optical, tapes and removable disk cartridge.
4	Solution shall support minimum of Representational State Transfer (REST), Common Internet File System (CIFS), and Network File System (NFS) protocol.

5	Solution shall provide an intelligent policy-based object storage system. Solution shall be fully automated, policy driven without manual intervention, script, or wizard based automation to manage data retention, replication, and data distribution policies. For example, if the policy is defined to have 1 copy of the data locally at the primary site and 1 copy of the data at the remote site. In the event when primary site is not able to communicate with the remote site due to a temporary outage at the remote site, the solution shall automatically create a temporary remote copy at a remote tertiary site intelligently or a user defined temporary remote tertiary location during the creation of the policy process to meet the policy requirement (1 local and 1 remote). When the communication to the original remote site is restored, the solution will update and re-synchronize the missing data automatically to the original remote site and automatically delete the temporary remote copy at the temporary remote tertiary location. The solution shall automatically perform self healing of the system during a non-disaster type of outage. An alert and logging mechanism shall be included in the solution to capture the sequence of activities and provide the final status via email to the designated recipient(s).
6	Solution shall provide customizable policy to define the number of synchronous local data copies, the number of asynchronous remote data copies, the number of sites to store the data, the primary site location, the disaster recover (DR) site location and the temporary remote tertiary site location.
7	The solution shall have the ability to provide automatic or user definable thresholds in the policy to determine temporary interruptions (such as system resource and/or communication problems) when accessing the DR site. This capability is used to determine when the remote copy of the data shall be copied to the temporary tertiary site.

8	The Contractor shall provide a single Graphic User Interface (GUI) that allows more than one creations, editions, and deletions of data retention, replication, and data distribution policies in a one single process. For example, data retention, replication, and data distribution policies can be configured in one GUI interface and not to have separate individual interfaces for data retention, replication, and data distribution respectively.
9	Solution shall replicate files to the remote site based on available WAN bandwidth and remote system resources. The process shall be fully automated, policy driven without manual intervention, script or wizard based automation.
10	Solution shall provide the necessary equipments at the secondary remote site so that the remote site can be promoted to primary site role in the event of total disaster at the primary site.
11	In the event of a site recovery, the solution shall be capable of creating a duplicate system by copying all data from the Disaster Recovery site which will be shipped to the disaster site to be recovered.
12	Solution shall provide storage capacity expansion or scalability with no downtime, no forklift upgrade, no reconfiguration of the internal operating system, and LUN remapping of the storage subsystem to connecting hosts. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
13	Solution shall support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
14	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.

15	Solution shall be able to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
16	Solution shall provide File Transfer ingest rate to local storage solution at a minimum of 1.5 Gigabytes (GB) of data per minute (1.5GB/min).
17	Shall Support a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis)
18	Solution shall always maintain original file attributes (Create, Access dates, file permission, and security or other attributes) for all data replication process, data copy process including data restoration processes. The file attributes are to stay with the file.
19	Solution shall provide the ability to verify data after it has been transferred from the local site to the remote location to ensure it matches with no data corruption. If verification of data fails solution shall resend the data. The copy of file at the remote site shall be identical to the copy of the image file at the local site after replication. This check shall be performed automatically.
20	Solution shall automatically (based on policy, not manual, script or wizard based) redirect the read processes to remote storage devices/components if the local storage devices/components are not available during image file read process.
21	Solution shall provide a solution that can automatically (based on policy, not manual, script or wizard based) redirect the write processes to remote storage node and/or backend storage if the local storage node and/or backend storage is not available during image file write process.

22	The solution shall present a CIFS interface that is addressable by a Microsoft Active Directory fully qualified path. The Solution shall present a redundant CIFS interface. It must be presented to any windows client on the network. Any windows client on the network must be able to authenticate to the server and access to the share.
23	The Contractor shall provide a redundant Global Namespace object based Archive system. All objects shall be retrievable via web browser (http and https) based on its object metadata definitions.
24	Solution shall maintain mappings of the Common Internet File System (CIFS) share in the event that the primary local gateway is unavailable or offline. The solution shall continue to function automatically with no manual intervention, script or wizard based automation on local secondary gateway with the same CIFS mapping. The path used to access the CIFS shares will be the same regardless of whether the local or remote copy of the image is accessed.
25	Solution shall provide a process automatically (based on policy, not manual, script or wizard based) update and resynchronize the recovered local site archive storage from the remote archive storage when the local archive storage is back online after a period of downtime. The process shall be fully automated, policy driven without manual intervention, script or wizard based automation
26	Solution shall provide a process to log all file transfer success or failure.
27	Solution shall utilize Microsoft Active Directory for all security permissions for the whole system management and data access.
28	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system components problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact

29	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and other similar components.
30	Solution shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process and SMTP mail.
31	Solution shall escalate alerts when storage space utilization falls below a user defined threshold.
32	Solution shall provide a means for the solution to log the file transfer time from local archive to remote site as a user defined threshold. (e.g. If logging transfer time is set to 60 seconds and the actual transfer time exceeds 60 seconds it shall be logged).
33	Solution shall support the function to access remote data from the local archive location for display purposes.
34	Solution shall provide a means for the Solution to retrieve a copy of the data from the remote archive locations for storage at the local archive location if the local archive was not available.
35	Solution shall log file access, create and modify dates for retention statistics and monitoring purposes.
36	Solution shall under normal operating conditions, replicate data immediately. In no case shall the replication backlog be greater than four (4) hours of data.
37	Solution shall be able to scale components such as network interface cards, adapter ports, processors, memory, and storage capacity independently.
38	Solution shall monitor and access the remote data with the least amount of file transfer latency.
39	Solution shall manage, control, and define policies (policy that defines the number of data replication copies, the location, and the temporary remote tertiary site location) in the Object storage device.
40	Solution shall be capable to capture and/or log performance data such as data ingest rate, data ingest size, data replication bandwidth utilization, data replication latency, data retrieval response time and others.
41	Solution shall support a minimum of two 1Gb Ethernet connectivity to the local production LAN.

42	Solution shall provide redundant Power Distribution Unit (PDUs) with sufficient outlets to power all units in the rack(s).																														
43	Solution equipment shall be Pre-installed and Pre-cabled in a 42U Rack prior to delivery. All cables and components installed in the rack shall be labeled.																														
44	Solution shall include Pre-installed and Pre-cabled redundant top of the rack network switches in every rack provided to minimize the number of network connections to VA Core network switches. The top of the rack switches provided in the solution shall be interoperable with existing VA Core network switches.																														
45	Solution shall support Internet Protocol version 6 (IPv6).																														
46	Solution shall support a minimum of the following file formats: <table> <tr> <td>AVI</td><td>Motion Video AVI</td></tr> <tr> <td>BMP</td><td>Bitmap file BMP</td></tr> <tr> <td>DCM</td><td>Dicom file DCM</td></tr> <tr> <td>HTML</td><td>Web Document HTML</td></tr> <tr> <td>JPG</td><td>Full Color JPG</td></tr> <tr> <td>MHTML</td><td>MIME HTML Document</td></tr> <tr> <td>MP3</td><td>Motion Video MPEG-3</td></tr> <tr> <td>MP4</td><td>Motion Video MPEG-4</td></tr> <tr> <td>MPG</td><td>Motion Video MPG</td></tr> <tr> <td>PDF</td><td>Adobe PDF</td></tr> <tr> <td>RTF</td><td>Rich Text format RTF</td></tr> <tr> <td>TGA</td><td>Targa Image TGA</td></tr> <tr> <td>TIF</td><td>Scanned Document TIF</td></tr> <tr> <td>TXT</td><td>Text file import TXT</td></tr> <tr> <td>WAV</td><td>Audio file WAV</td></tr> </table>	AVI	Motion Video AVI	BMP	Bitmap file BMP	DCM	Dicom file DCM	HTML	Web Document HTML	JPG	Full Color JPG	MHTML	MIME HTML Document	MP3	Motion Video MPEG-3	MP4	Motion Video MPEG-4	MPG	Motion Video MPG	PDF	Adobe PDF	RTF	Rich Text format RTF	TGA	Targa Image TGA	TIF	Scanned Document TIF	TXT	Text file import TXT	WAV	Audio file WAV
AVI	Motion Video AVI																														
BMP	Bitmap file BMP																														
DCM	Dicom file DCM																														
HTML	Web Document HTML																														
JPG	Full Color JPG																														
MHTML	MIME HTML Document																														
MP3	Motion Video MPEG-3																														
MP4	Motion Video MPEG-4																														
MPG	Motion Video MPG																														
PDF	Adobe PDF																														
RTF	Rich Text format RTF																														
TGA	Targa Image TGA																														
TIF	Scanned Document TIF																														
TXT	Text file import TXT																														
WAV	Audio file WAV																														
47	Solution shall make the file transfer process transparent to end users with no user intervention needed. The physical location of the data repository shall be transparent to end user.																														
48	Solution shall perform automatic restoration of a corrupted file (Object/File Data and Meta Data) from a Disaster Recovery (DR) copy.																														
49	Solution shall automatically resume or recover from file transfer failures.																														

50	Solution shall provide capability to log events and problems and provide the ability to manually set the level of logging and reporting.
51	Solution shall provide a role based configuration with a minimum of a system user role which allows for a system user to view current hardware status and a Super User system administration role which allows for an administrator to configure system policies, and parameters.
52	Solution shall provide a web based single master management administrative console without the need to install client software for control of system software implementation, policies and user management protected with permission roles.
53	Solution shall utilize Microsoft Active Directory to provide a single sign-on to the management web console and the log on security shall provide the permission to access and manage all the CIFS shares and data.
54	Solution shall log the software version/installed hardware/firmware versions at each site.
55	Solution shall provide interface callable from an application using HTTP/S Web Services using SOAP or REST and Get/Post methods for moving binary data. The ICD/WSDL will be included with the solution.
56	Solution shall provide a web interface to access the metadata of the files/objects that are stored in the storage device.
57	Solution shall provide web interface to access the system logs generated by all components. If separate logs are generated the interface will include the ability to determine what logs are available and parameters to select specific logs.
58	Solution shall provide a web interface to access files by file path/name.
59	Solution shall provide a web interface to store files by file path/name.
60	Solution shall provide Web interface that provides usage statistics (metrics on all nodes –size, amount full, number of files, as examples).
61	Solution shall provide web interface that provides access to the list of files by attributes (MIME type, date created/range, size, file name or partial file name).

62	Solution shall provide a web interface that will export/copy files by attributes (e.g. File path or partial file path) to a specified target CFIS Share.
63	Solution shall provide a web interface that provides file statistics (e.g., size, creation date, modify date, access date) given File name or file path, or File/Object ID specified by the solution.
64	Solution shall provide web interface that provides image retrieval time statistics given an Object/File ID or file path.
65	Solution shall provide a web interface that provides the "Health status" of the storage (i.e. what is the current status of each of the nodes on the network or of a particular node).
66	Solution shall provide a web interface that provides status of devices (e.g. any disk errors or outages.)
67	Solution shall provide web interface that provides the physical location of Storage devices given a device ID supplied by the vendor, or the list of storage devices and characteristics for all devices at a location.

GRID Based Object Storage (Large)	
OEM Model/Part Number:	
Reference Number	Requirements
1	Solution shall provide minimum usable native disk capacity without data compression, without data deduplication, and without single instance (no duplicate objects) of 100TB (Terabytes), expandable to a maximum of 200TB (Terabytes).
2	Solution shall provide a minimum of Enterprise grade SATA spinning disks or better as the backend storage devices to store the object data.
3	The solution shall not include removable media, such as optical, tapes and removable disk cartridge.
4	Solution shall support minimum of Representational State Transfer (REST), Common Internet File System (CIFS), and Network File System (NFS) protocol.

5	Solution shall provide an intelligent policy-based object storage system. Solution shall be fully automated, policy driven without manual intervention, script, or wizard based automation to manage data retention, replication, and data distribution policies. For example, if the policy is defined to have 1 copy of the data locally at the primary site and 1 copy of the data at the remote site. In the event when primary site is not able to communicate with the remote site due to a temporary outage at the remote site, the solution shall automatically create a temporary remote copy at a remote tertiary site intelligently or a user defined temporary remote tertiary location during the creation of the policy process to meet the policy requirement (1 local and 1 remote). When the communication to the original remote site is restored, the solution will update and re-synchronize the missing data automatically to the original remote site and automatically delete the temporary remote copy at the temporary remote tertiary location. The solution shall automatically perform self healing of the system during a non-disaster type of outage. An alert and logging mechanism shall be included in the solution to capture the sequence of activities and provide the final status via email to the designated recipient(s).
6	Solution shall provide customizable policy to define the number of synchronous local data copies, the number of asynchronous remote data copies, the number of sites to store the data, the primary site location, the disaster recover (DR) site location and the temporary remote tertiary site location.
7	The solution shall have the ability to provide automatic or user definable thresholds in the policy to determine temporary interruptions (such as system resource and/or communication problems) when accessing the DR site. This capability is used to determine when the remote copy of the data shall be copied to the temporary tertiary site.

8	The Contractor shall provide a single Graphic User Interface (GUI) that allows more than one creations, editions, and deletions of data retention, replication, and data distribution policies in a one single process. For example, data retention, replication, and data distribution policies can be configured in one GUI interface and not to have separate individual interfaces for data retention, replication, and data distribution respectively.
9	Solution shall replicate files to the remote site based on available WAN bandwidth and remote system resources. The process shall be fully automated, policy driven without manual intervention, script or wizard based automation.
10	Solution shall provide the necessary equipments at the secondary remote site so that the remote site can be promoted to primary site role in the event of total disaster at the primary site.
11	In the event of a site recovery, the solution shall be capable of creating a duplicate system by copying all data from the Disaster Recovery site which will be shipped to the disaster site to be recovered.
12	Solution shall provide storage capacity expansion or scalability with no downtime, no forklift upgrade, no reconfiguration of the internal operating system, and LUN remapping of the storage subsystem to connecting hosts. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
13	Solution shall support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
14	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.

15	Solution shall be able to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
16	Solution shall provide File Transfer ingest rate to local storage solution at a minimum of 1.5 Gigabytes (GB) of data per minute (1.5GB/min).
17	Shall Support a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis)
18	Solution shall always maintain original file attributes (Create, Access dates, file permission, and security or other attributes) for all data replication process, data copy process including data restoration processes. The file attributes are to stay with the file.
19	Solution shall provide the ability to verify data after it has been transferred from the local site to the remote location to ensure it matches with no data corruption. If verification of data fails solution shall resend the data. The copy of file at the remote site shall be identical to the copy of the image file at the local site after replication. This check shall be performed automatically.
20	Solution shall automatically (based on policy, not manual, script or wizard based) redirect the read processes to remote storage devices/components if the local storage devices/components are not available during image file read process.
21	Solution shall provide a solution that can automatically (based on policy, not manual, script or wizard based) redirect the write processes to remote storage node and/or backend storage if the local storage node and/or backend storage is not available during image file write process.

22	The solution shall present a CIFS interface that is addressable by a Microsoft Active Directory fully qualified path. The Solution shall present a redundant CIFS interface. It must be presented to any windows client on the network. Any windows client on the network must be able to authenticate to the server and access to the share.
23	The Contractor shall provide a redundant Global Namespace object based Archive system. All objects shall be retrievable via web browser (http and https) based on its object metadata definitions.
24	Solution shall maintain mappings of the Common Internet File System (CIFS) share in the event that the primary local gateway is unavailable or offline. The solution shall continue to function automatically with no manual intervention, script or wizard based automation on local secondary gateway with the same CIFS mapping. The path used to access the CIFS shares will be the same regardless of whether the local or remote copy of the image is accessed.
25	Solution shall provide a process automatically (based on policy, not manual, script or wizard based) update and resynchronize the recovered local site archive storage from the remote archive storage when the local archive storage is back online after a period of downtime. The process shall be fully automated, policy driven without manual intervention, script or wizard based automation
26	Solution shall provide a process to log all file transfer success or failure.
27	Solution shall utilize Microsoft Active Directory for all security permissions for the whole system management and data access.
28	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system components problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact

29	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and other similar components.
30	Solution shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process and SMTP mail.
31	Solution shall escalate alerts when storage space utilization falls below a user defined threshold.
32	Solution shall provide a means for the solution to log the file transfer time from local archive to remote site as a user defined threshold. (e.g. If logging transfer time is set to 60 seconds and the actual transfer time exceeds 60 seconds it shall be logged).
33	Solution shall support the function to access remote data from the local archive location for display purposes.
34	Solution shall provide a means for the Solution to retrieve a copy of the data from the remote archive locations for storage at the local archive location if the local archive was not available.
35	Solution shall log file access, create and modify dates for retention statistics and monitoring purposes.
36	Solution shall under normal operating conditions, replicate data immediately. In no case shall the replication backlog be greater than four (4) hours of data.
37	Solution shall be able to scale components such as network interface cards, adapter ports, processors, memory, and storage capacity independently.
38	Solution shall monitor and access the remote data with the least amount of file transfer latency.
39	Solution shall manage, control, and define policies (policy that defines the number of data replication copies, the location, and the temporary remote tertiary site location) in the Object storage device.
40	Solution shall be capable to capture and/or log performance data such as data ingest rate, data ingest size, data replication bandwidth utilization, data replication latency, data retrieval response time and others.
41	Solution shall support a minimum of two 1Gb Ethernet connectivity to the local production LAN.

42	Solution shall provide redundant Power Distribution Unit (PDUs) with sufficient outlets to power all units in the rack(s).																														
43	Solution equipment shall be Pre-installed and Pre-cabled in a 42U Rack prior to delivery. All cables and components installed in the rack shall be labeled.																														
44	Solution shall include Pre-installed and Pre-cabled redundant top of the rack network switches in every rack provided to minimize the number of network connections to VA Core network switches. The top of the rack switches provided in the solution shall be interoperable with existing VA Core network switches.																														
45	Solution shall support Internet Protocol version 6 (IPv6).																														
46	Solution shall support a minimum of the following file formats: <table> <tr> <td>AVI</td><td>Motion Video AVI</td></tr> <tr> <td>BMP</td><td>Bitmap file BMP</td></tr> <tr> <td>DCM</td><td>Dicom file DCM</td></tr> <tr> <td>HTML</td><td>Web Document HTML</td></tr> <tr> <td>JPG</td><td>Full Color JPG</td></tr> <tr> <td>MHTML</td><td>MIME HTML Document</td></tr> <tr> <td>MP3</td><td>Motion Video MPEG-3</td></tr> <tr> <td>MP4</td><td>Motion Video MPEG-4</td></tr> <tr> <td>MPG</td><td>Motion Video MPG</td></tr> <tr> <td>PDF</td><td>Adobe PDF</td></tr> <tr> <td>RTF</td><td>Rich Text format RTF</td></tr> <tr> <td>TGA</td><td>Targa Image TGA</td></tr> <tr> <td>TIF</td><td>Scanned Document TIF</td></tr> <tr> <td>TXT</td><td>Text file import TXT</td></tr> <tr> <td>WAV</td><td>Audio file WAV</td></tr> </table>	AVI	Motion Video AVI	BMP	Bitmap file BMP	DCM	Dicom file DCM	HTML	Web Document HTML	JPG	Full Color JPG	MHTML	MIME HTML Document	MP3	Motion Video MPEG-3	MP4	Motion Video MPEG-4	MPG	Motion Video MPG	PDF	Adobe PDF	RTF	Rich Text format RTF	TGA	Targa Image TGA	TIF	Scanned Document TIF	TXT	Text file import TXT	WAV	Audio file WAV
AVI	Motion Video AVI																														
BMP	Bitmap file BMP																														
DCM	Dicom file DCM																														
HTML	Web Document HTML																														
JPG	Full Color JPG																														
MHTML	MIME HTML Document																														
MP3	Motion Video MPEG-3																														
MP4	Motion Video MPEG-4																														
MPG	Motion Video MPG																														
PDF	Adobe PDF																														
RTF	Rich Text format RTF																														
TGA	Targa Image TGA																														
TIF	Scanned Document TIF																														
TXT	Text file import TXT																														
WAV	Audio file WAV																														
47	Solution shall make the file transfer process transparent to end users with no user intervention needed. The physical location of the data repository shall be transparent to end user.																														
48	Solution shall perform automatic restoration of a corrupted file (Object/File Data and Meta Data) from a Disaster Recovery (DR) copy.																														
49	Solution shall automatically resume or recover from file transfer failures.																														

50	Solution shall provide capability to log events and problems and provide the ability to manually set the level of logging and reporting.
51	Solution shall provide a role based configuration with a minimum of a system user role which allows for a system user to view current hardware status and a Super User system administration role which allows for an administrator to configure system policies, and parameters.
52	Solution shall provide a web based single master management administrative console without the need to install client software for control of system software implementation, policies and user management protected with permission roles.
53	Solution shall utilize Microsoft Active Directory to provide a single sign-on to the management web console and the log on security shall provide the permission to access and manage all the CIFS shares and data.
54	Solution shall log the software version/installed hardware/firmware versions at each site.
55	Solution shall provide interface callable from an application using HTTP/S Web Services using SOAP or REST and Get/Post methods for moving binary data. The ICD/WSDL will be included with the solution.
56	Solution shall provide a web interface to access the metadata of the files/objects that are stored in the storage device.
57	Solution shall provide web interface to access the system logs generated by all components. If separate logs are generated the interface will include the ability to determine what logs are available and parameters to select specific logs.
58	Solution shall provide a web interface to access files by file path/name.
59	Solution shall provide a web interface to store files by file path/name.
60	Solution shall provide Web interface that provides usage statistics (metrics on all nodes –size, amount full, number of files, as examples).
61	Solution shall provide web interface that provides access to the list of files by attributes (MIME type, date created/range, size, file name or partial file name).

62	Solution shall provide a web interface that will export/copy files by attributes (e.g. File path or partial file path) to a specified target CFIS Share.
63	Solution shall provide a web interface that provides file statistics (e.g., size, creation date, modify date, access date) given File name or file path, or File/Object ID specified by the solution.
64	Solution shall provide web interface that provides image retrieval time statistics given an Object/File ID or file path.
65	Solution shall provide a web interface that provides the "Health status" of the storage (i.e. what is the current status of each of the nodes on the network or of a particular node).
66	Solution shall provide a web interface that provides status of devices (e.g. any disk errors or outages.)
67	Solution shall provide web interface that provides the physical location of Storage devices given a device ID supplied by the vendor, or the list of storage devices and characteristics for all devices at a location.

	GRID Based Object Storage (Extra Large)
	OEM Model/Part Number:
Reference Number	Requirements
1	Solution shall provide minimum usable native disk capacity without data compression, without data deduplication, and without single instance (no duplicate objects) of 200TB (Terabytes), expandable to at least 500TB (Terabytes).
2	Solution shall provide a minimum of Enterprise grade SATA spinning disks or better as the backend storage devices to store the object data.
3	The solution shall not include removable media, such as optical, tapes and removable disk cartridge.
4	Solution shall support minimum of Representational State Transfer (REST), Common Internet File System (CIFS), and Network File System (NFS) protocol.

5	Solution shall provide an intelligent policy-based object storage system. Solution shall be fully automated, policy driven without manual intervention, script, or wizard based automation to manage data retention, replication, and data distribution policies. For example, if the policy is defined to have 1 copy of the data locally at the primary site and 1 copy of the data at the remote site. In the event when primary site is not able to communicate with the remote site due to a temporary outage at the remote site, the solution shall automatically create a temporary remote copy at a remote tertiary site intelligently or a user defined temporary remote tertiary location during the creation of the policy process to meet the policy requirement (1 local and 1 remote). When the communication to the original remote site is restored, the solution will update and re-synchronize the missing data automatically to the original remote site and automatically delete the temporary remote copy at the temporary remote tertiary location. The solution shall automatically perform self healing of the system during a non-disaster type of outage. An alert and logging mechanism shall be included in the solution to capture the sequence of activities and provide the final status via email to the designated recipient(s).
6	Solution shall provide customizable policy to define the number of synchronous local data copies, the number of asynchronous remote data copies, the number of sites to store the data, the primary site location, the disaster recover (DR) site location and the temporary remote tertiary site location.
7	The solution shall have the ability to provide automatic or user definable thresholds in the policy to determine temporary interruptions (such as system resource and/or communication problems) when accessing the DR site. This capability is used to determine when the remote copy of the data shall be copied to the temporary tertiary site.

8	The Contractor shall provide a single Graphic User Interface (GUI) that allows more than one creations, editions, and deletions of data retention, replication, and data distribution policies in a one single process. For example, data retention, replication, and data distribution policies can be configured in one GUI interface and not to have separate individual interfaces for data retention, replication, and data distribution respectively.
9	Solution shall replicate files to the remote site based on available WAN bandwidth and remote system resources. The process shall be fully automated, policy driven without manual intervention, script or wizard based automation.
10	Solution shall provide the necessary equipments at the secondary remote site so that the remote site can be promoted to primary site role in the event of total disaster at the primary site.
11	In the event of a site recovery, the solution shall be capable of creating a duplicate system by copying all data from the Disaster Recovery site which will be shipped to the disaster site to be recovered.
12	Solution shall provide storage capacity expansion or scalability with no downtime, no forklift upgrade, no reconfiguration of the internal operating system, and LUN remapping of the storage subsystem to connecting hosts. Any expansion shall maintain the same redundancy, performance and efficiency of the system as the initial delivered system exhibits on all supported protocols.
13	Solution shall support redundancy in all storage system components with no single point of failure and non-disruptive to operations for all system component replacements or repairs or firmware and microcode upgrades or updates.
14	Solution shall provide an automatic mechanism to migrate data from existing storage to any future new storage device when the storage hardware is End-of-life (EOL) with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.

15	Solution shall be able to migrate data to newer types of disk drive when replacing end-of-support disks with no impact to production operations, no downtime, and shall provide access to old and new storage data at all times during the migration process.
16	Solution shall provide File Transfer ingest rate to local storage solution at a minimum of 1.5 Gigabytes (GB) of data per minute (1.5GB/min).
17	Shall Support a minimum of five nines storage subsystem uptime (or 99.999% availability, excluding planned downtime). (Note: Five Nines (99.999%) = 5.3 minutes of downtime on a rolling 12 month basis)
18	Solution shall always maintain original file attributes (Create, Access dates, file permission, and security or other attributes) for all data replication process, data copy process including data restoration processes. The file attributes are to stay with the file.
19	Solution shall provide the ability to verify data after it has been transferred from the local site to the remote location to ensure it matches with no data corruption. If verification of data fails solution shall resend the data. The copy of file at the remote site shall be identical to the copy of the image file at the local site after replication. This check shall be performed automatically.
20	Solution shall automatically (based on policy, not manual, script or wizard based) redirect the read processes to remote storage devices/components if the local storage devices/components are not available during image file read process.
21	Solution shall provide a solution that can automatically (based on policy, not manual, script or wizard based) redirect the write processes to remote storage node and/or backend storage if the local storage node and/or backend storage is not available during image file write process.

22	The solution shall present a CIFS interface that is addressable by a Microsoft Active Directory fully qualified path. The Solution shall present a redundant CIFS interface. It must be presented to any windows client on the network. Any windows client on the network must be able to authenticate to the server and access to the share.
23	The Contractor shall provide a redundant Global Namespace object based Archive system. All objects shall be retrievable via web browser (http and https) based on its object metadata definitions.
24	Solution shall maintain mappings of the Common Internet File System (CIFS) share in the event that the primary local gateway is unavailable or offline. The solution shall continue to function automatically with no manual intervention, script or wizard based automation on local secondary gateway with the same CIFS mapping. The path used to access the CIFS shares will be the same regardless of whether the local or remote copy of the image is accessed.
25	Solution shall provide a process automatically (based on policy, not manual, script or wizard based) update and resynchronize the recovered local site archive storage from the remote archive storage when the local archive storage is back online after a period of downtime. The process shall be fully automated, policy driven without manual intervention, script or wizard based automation
26	Solution shall provide a process to log all file transfer success or failure.
27	Solution shall utilize Microsoft Active Directory for all security permissions for the whole system management and data access.
28	Shall provide native capability to proactively monitor/manage hardware and software processing, and generate alerts on potential storage system components problems, failures and application storage resources health. This information should be capable of being transmitted to the OEM or Vendor as defined by the contract and designated VA Point of Contact

29	Shall provide native capability to report or generate reports at a minimum on hardware failures or items out-of-specifications in the Storage Subsystem, such as Disk Drives, Fans or Power Supplies and other similar components.
30	Solution shall have a native alert function to send failures/warnings/alerts via a "Call Home" function or similar process and SMTP mail.
31	Solution shall escalate alerts when storage space utilization falls below a user defined threshold.
32	Solution shall provide a means for the solution to log the file transfer time from local archive to remote site as a user defined threshold. (e.g. If logging transfer time is set to 60 seconds and the actual transfer time exceeds 60 seconds it shall be logged).
33	Solution shall support the function to access remote data from the local archive location for display purposes.
34	Solution shall provide a means for the Solution to retrieve a copy of the data from the remote archive locations for storage at the local archive location if the local archive was not available.
35	Solution shall log file access, create and modify dates for retention statistics and monitoring purposes.
36	Solution shall under normal operating conditions, replicate data immediately. In no case shall the replication backlog be greater than four (4) hours of data.
37	Solution shall be able to scale components such as network interface cards, adapter ports, processors, memory, and storage capacity independently.
38	Solution shall monitor and access the remote data with the least amount of file transfer latency.
39	Solution shall manage, control, and define policies (policy that defines the number of data replication copies, the location, and the temporary remote tertiary site location) in the Object storage device.
40	Solution shall be capable to capture and/or log performance data such as data ingest rate, data ingest size, data replication bandwidth utilization, data replication latency, data retrieval response time and others.
41	Solution shall support a minimum of two 1Gb Ethernet connectivity to the local production LAN.

42	Solution shall provide redundant Power Distribution Unit (PDUs) with sufficient outlets to power all units in the rack(s).																														
43	Solution equipment shall be Pre-installed and Pre-cabled in a 42U Rack prior to delivery. All cables and components installed in the rack shall be labeled.																														
44	Solution shall include Pre-installed and Pre-cabled redundant top of the rack network switches in every rack provided to minimize the number of network connections to VA Core network switches. The top of the rack switches provided in the solution shall be interoperable with existing VA Core network switches.																														
45	Solution shall support Internet Protocol version 6 (IPv6).																														
46	Solution shall support a minimum of the following file formats: <table> <tr> <td>AVI</td><td>Motion Video AVI</td></tr> <tr> <td>BMP</td><td>Bitmap file BMP</td></tr> <tr> <td>DCM</td><td>Dicom file DCM</td></tr> <tr> <td>HTML</td><td>Web Document HTML</td></tr> <tr> <td>JPG</td><td>Full Color JPG</td></tr> <tr> <td>MHTML</td><td>MIME HTML Document</td></tr> <tr> <td>MP3</td><td>Motion Video MPEG-3</td></tr> <tr> <td>MP4</td><td>Motion Video MPEG-4</td></tr> <tr> <td>MPG</td><td>Motion Video MPG</td></tr> <tr> <td>PDF</td><td>Adobe PDF</td></tr> <tr> <td>RTF</td><td>Rich Text format RTF</td></tr> <tr> <td>TGA</td><td>Targa Image TGA</td></tr> <tr> <td>TIF</td><td>Scanned Document TIF</td></tr> <tr> <td>TXT</td><td>Text file import TXT</td></tr> <tr> <td>WAV</td><td>Audio file WAV</td></tr> </table>	AVI	Motion Video AVI	BMP	Bitmap file BMP	DCM	Dicom file DCM	HTML	Web Document HTML	JPG	Full Color JPG	MHTML	MIME HTML Document	MP3	Motion Video MPEG-3	MP4	Motion Video MPEG-4	MPG	Motion Video MPG	PDF	Adobe PDF	RTF	Rich Text format RTF	TGA	Targa Image TGA	TIF	Scanned Document TIF	TXT	Text file import TXT	WAV	Audio file WAV
AVI	Motion Video AVI																														
BMP	Bitmap file BMP																														
DCM	Dicom file DCM																														
HTML	Web Document HTML																														
JPG	Full Color JPG																														
MHTML	MIME HTML Document																														
MP3	Motion Video MPEG-3																														
MP4	Motion Video MPEG-4																														
MPG	Motion Video MPG																														
PDF	Adobe PDF																														
RTF	Rich Text format RTF																														
TGA	Targa Image TGA																														
TIF	Scanned Document TIF																														
TXT	Text file import TXT																														
WAV	Audio file WAV																														
47	Solution shall make the file transfer process transparent to																														
48	Solution shall perform automatic restoration of a corrupted file (Object/File Data and Meta Data) from a Disaster Recovery (DR) copy.																														
49	Solution shall automatically resume or recover from file transfer failures.																														
50	Solution shall provide capability to log events and problems and provide the ability to manually set the level of logging and reporting.																														

51	Solution shall provide a role based configuration with a minimum of a system user role which allows for a system user to view current hardware status and a Super User system administration role which allows for an administrator to configure system policies, and parameters.
52	Solution shall provide a web based single master management administrative console without the need to install client software for control of system software implementation, policies and user management protected with permission roles.
53	Solution shall utilize Microsoft Active Directory to provide a single sign-on to the management web console and the log on security shall provide the permission to access and manage all the CIFS shares and data.
54	Solution shall log the software version/installed hardware/firmware versions at each site.
55	Solution shall provide interface callable from an application using HTTP/S Web Services using SOAP or REST and Get/Post methods for moving binary data. The ICD/WSDL will be included with the solution.
56	Solution shall provide a web interface to access the metadata of the files/objects that are stored in the storage device.
57	Solution shall provide web interface to access the system logs generated by all components. If separate logs are generated the interface will include the ability to determine what logs are available and parameters to select specific logs.
58	Solution shall provide a web interface to access files by file path/name.
59	Solution shall provide a web interface to store files by file path/name.
60	Solution shall provide Web interface that provides usage statistics (metrics on all nodes –size, amount full, number of files, as examples).
61	Solution shall provide web interface that provides access to the list of files by attributes (MIME type, date created/range, size, file name or partial file name).
62	Solution shall provide a web interface that will export/copy files by attributes (e.g. File path or partial file path) to a specified target CFIS Share.

63	Solution shall provide a web interface that provides file statistics (e.g., size, creation date, modify date, access date) given File name or file path, or File/Object ID specified by the solution.
64	Solution shall provide web interface that provides image retrieval time statistics given an Object/File ID or file path.
65	Solution shall provide a web interface that provides the "Health status" of the storage (i.e. what is the current status of each of the nodes on the network or of a particular node).
66	Solution shall provide a web interface that provides status of devices (e.g. any disk errors or outages.)
67	Solution shall provide web interface that provides the physical location of Storage devices given a device ID supplied by the vendor, or the list of storage devices and characteristics for all devices at a location.

Perimeter Gateway Security Device	
	OEM & Model/Part Number:
Parameter	Requirement
Interfaces	Minimum: Qty (10) 1 Gigabit Copper/Fiber
	Minimum: Qty (4) 10 Gigabit SFP+
	Minimum Management: Qty (1) 100/1000 Copper
	Minimum Console: Qty (1)
Power	Redundant power supplies
	Follows NEMA standards
Performance	Minimum Throughput (Multi-protocol): 20 Gbps Full-Duplex
	Minimum Concurrent Sessions: 3,000,000
	Minimum Number of Supported VLANs: 1,024
	Minimum Number of Supported Access Control Entries (ACEs): 250,000 (per context)
	Minimum Virtual Instances: 100
Required Features	High Availability: A/P, A/A
	Routing: Static, OSPFv3
	IPv4/IPv6
	802.1q
	Link Aggregation
	Auto-duplex interface capabilities
	Layer 2 Transparent, Layer 3 Routed, Virtualized Layer 2, Virtualized Layer 3 Modes
	Low impact chassis cluster upgrades
	Configuration synchronization
	Session synchronization for firewall
	Device failure detection
	Link and upstream failure detection
	Dual control links (session + state)
	Active-Standby stateful failover
	Active-Active stateful failover support in multiple context mode; Session failover for routing change
	Scalability: Cluster or Load Balancing
	Network Address Translation (NAT)
	Port Address Translation (PAT)
	Syslog
	ACL Logging (Buffered and Remote)
	Resource management controls resource usage per security context
	Dynamic port allocation
	Protocol state tracking
Management	SSHv2 to CLI
	Web GUI-based single device manager (HTTPS)
	SNMP v2c MIBs and traps, SNMPv3
	Authentication, authorization, and accounting (AAA): RADIUS support
	Role-based administrative access
	Online upgrade
	Support for two-factor authentication

Mid-Range Internal Security Device	
	OEM & Model/Part Number:
Parameter	Requirement
Interfaces	Minimum: Qty (6) 1 Gigabit Copper/Fiber
	Minimum: Qty (2) 10 Gigabit SFP+
	Minimum Management: Qty (1) 100/1000 Copper
	Minimum Console: Qty (1)
Power	Redundant power supplies
	Follows NEMA standards
Performance	Minimum Throughput (Multi-protocol): 20 Gbps Full-Duplex
	Minimum Concurrent Sessions: 3,000,000
	Minimum Number of Supported VLANs: 1,024
	Minimum Number of Supported Access Control Entries (ACEs): 125,000 (per context)
	Minimum Virtual Instances: 20
Required Features	High Availability: A/P, A/A
	Routing: Static, OSPFv3
	IPv4/IPv6
	802.1q
	Link Aggregation
	Auto-duplex interface capabilities
	Layer 2 Transparent, Layer 3 Routed, Virtualized Layer 2, Virtualized Layer 3 Modes
	Low impact chassis cluster upgrades
	Configuration synchronization
	Session synchronization for firewall
	Device failure detection
	Link and upstream failure detection
	Dual control links (session + state)
	Active-Standby stateful failover
	Active-Active stateful failover support in multiple context mode; Session failover for routing change
	Scalability: Cluster or Load Balancing
	Network Address Translation (NAT)
	Port Address Translation (PAT)
	Syslog
	ACL Logging (Buffered and Remote)
	Resource management controls resource usage per security context
	Dynamic port allocation
	Protocol state tracking
Management	SSHv2 to CLI
	Web GUI-based single device manager (HTTPS)
	SNMP v2c MIBs and traps, SNMPv3
	Authentication, authorization, and accounting (AAA): RADIUS support
	Role-based administrative access
	Online upgrade
	Support for two-factor authentication

Service Security Device	
	OEM & Model/Part Number:
Parameter	Requirement
Interfaces	Minimum: Qty (2) 1 Gigabit Copper/Fiber
	Minimum: Qty (0) 10 Gigabit SFP+
	Minimum Management: Qty (1) 100/1000 Copper
	Minimum Console: Qty (1)
Power	Single power supply
	Follows NEMA standards
Performance	Minimum Throughput (Multi-protocol): 10 Gbps Full-Duplex
	Minimum Concurrent Sessions: 1,000,000
	Minimum Number of Supported VLANs: 1,024
	Minimum Number of Supported Access Control Entries (ACEs): 50,000 (per context)
	Minimum Virtual Instances: 5
Required Features	High Availability: A/P, A/A
	Routing: Static, OSPFv3
	IPv4/IPv6
	802.1q
	Link Aggregation
	Auto-duplex interface capabilities
	Layer 2 Transparent, Layer 3 Routed, Virtualized Layer 2, Virtualized Layer 3 Modes
	Low impact chassis cluster upgrades
	Configuration synchronization
	Session synchronization for firewall
	Device failure detection
	Link and upstream failure detection
	Dual control links (session + state)
	Active-Standby stateful failover
	Active-Active stateful failover support in multiple context mode; Session failover for routing change
	Scalability: Cluster or Load Balancing
	Network Address Translation (NAT)
	Port Address Translation (PAT)
	Syslog
	ACL Logging (Buffered and Remote)
	Resource management controls resource usage per security context
	Dynamic port allocation
	Protocol state tracking
	VoIP Aware, SIP, SCCP
Management	SSHv2 to CLI
	Web GUI-based single device manager (HTTPS)
	SNMP v2c MIBs and traps, SNMPv3
	Authentication, authorization, and accounting (AAA): RADIUS support
	Role-based administrative access
	Online upgrade
	Support for two-factor authentication

The scope of this diagram is to show the efforts taken for repair of equipment for items covered within the Period of Performance and Terms & Conditions of the warranty

CEC Call Flow

Full Workflow

10/31/2011

