Contract # AR2493

STATE OF UTAH COOPERATIVE CONTRACT

1. CONTRACTING PARTIES: This contract is between the Division of Purchasing and the following Contractor:

VMware, Inc.
Name
12100 Sunset Hills Road, Suite 600
Address
Reston | Virginia | 20190
City | State | Zip

LEGAL STATUS OF CONTRACTOR
- ☐ Sole Proprietor
- ☐ Non-Profit Corporation
- ☒ For-Profit Corporation
- ☐ Partnership
- ☐ Government Agency

Contact Person Karin Whitwood Phone #571-375-3481 Email NASPO-VP@vmware.com
Vendor #115818A Commodity Code #920-05

2. GENERAL PURPOSE OF CONTRACT: Contractor is permitted to provide the Cloud Solutions identified in Attachment B to Participating States once a Participating Addendum has been signed

3. PROCUREMENT PROCESS: This contract is entered into as a result of the procurement process on Bid#CH16012.

4. CONTRACT PERIOD: Effective Date: 04/10/2017 Termination Date: 09/15/2026 unless terminated early or extended in accordance with the terms and conditions of this contract. Note: Pursuant to Solicitation #CH16012, Contract must re-certify its qualifications each year.

5. Administrative Fee, as described in the Solicitation and Attachment A: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.

6. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Pricing Schedule
ATTACHMENT D: Contractor's Response to Solicitation #CH16012

Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

8. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
   b. Utah State Procurement Code and the Procurement Rules.

9. Each signatory below represents that he or she has the requisite authority to enter into this contract.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

Contractor's signature — April 7, 2017 Date

Karin Whitwood, Contracts Manager, Public Sector
Type or Print Name and Title

STATE

Director, Division of Purchasing — 4/12/17 Date

Christopher Hughes	801-538-3254	801-538-3882	christopherhughes@utah.gov
Division of Purchasing Contact Person	Telephone Number	Fax Number	Email

(Revision 16 June 2016)

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

(1) A Participating Entity's Participating Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits[2] to the Master Agreement;
(3) The Solicitation;
(4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
(5) A Service Level Agreement issued against the Participating Addendum.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

2. Definitions - Unless otherwise provided in this Master Agreement, capitalized terms will have the meanings given to those terms in this Section.

Confidential Information means any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity.

Contractor means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees.

Data means all information, whether in oral or written (including electronic) form, created by or in any way originating with a Participating Entity or Purchasing Entity, and all information that is the output of any computer processing, or other electronic

[1] A Sample Participating Addendum will be published after the contracts have been awarded.
[2] The Exhibits comprise the terms and conditions for the service models: SaaS, IaaS, and PaaS.

manipulation, of any information that was created by or in any way originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Agreement.

Data Breach means any actual non-authorized access to or acquisition of computerized Non-Public Data or Personal Data that compromises the security, confidentiality, or integrity of the Non-Public Data or Personal Data, or the ability of Purchasing Entity to access the Non-Public Data or Personal Data.

Data Categorization means the process of risk assessment of Data. See also “High Risk Data”, “Moderate Risk Data” and “Low Risk Data”.

Disabling Code means computer instructions or programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, worms, date bombs or time bombs), including but not limited to other programs, data storage, computer libraries and programs that self-replicate without manual intervention, instructions programmed to activate at a predetermined time or upon a specified event, and/or programs purporting to do a meaningful function but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the Purchasing Entity’s’ software, applications and/or its end users processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating.

Fulfillment Partner means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Services under this Master Agreement and billing Customers directly for such Services. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

High Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“High Impact Data”).

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

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar

proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering the solicitation and any resulting Master Agreement(s).

Low Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Low Impact Data").

Master Agreement means this agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor, as now or hereafter amended.

Moderate Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Moderate Impact Data").

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

Non-Public Data means High Risk Data and Moderate Risk Data that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the Purchasing Entity because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Order means a purchase order, enterprise license agreement, or other ordering document issued by a Purchasing Entity to Contractor or a Fulfilment Partner that references and incorporates this Master Agreement.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate. Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

Personal Data means data alone or in combination that includes information relating to an individual that identifies the individual by name, identifying number, mark or description can be readily associated with a particular individual and which is not a public record. Personal Information may include the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person.

Platform as a Service (PaaS) as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Product means any deliverable under this Master Agreement, a Participating Addendum or Order, including Contractor's IaaS and SaaS offerings and/or software, reports, analyses, scripts, templates, code or other work results.

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes individually identifiable health information in: i) education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, ii) records described at 20 U.S.C. 1232g(a)(4)(B)(iv) iii) employment records held by a covered entity in its role as employer and iv) regarding a person who has been deceased for more than 50 years. Individually identifiable health information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Purchasing Entity means a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

Services mean any of the specifications described in the Scope of Services that are supplied or created by the Contractor pursuant to this Master Agreement.

Security Incident means a major security breach to the Contractor's system, which Contractor believes has resulted in an actual access to, use or disclosure or theft of a Purchasing Entity's Non-Public Data. A Security Incident may or may not turn into a Data Breach.

Service Level Agreement (SLA) means Contractor's standard SLAs as applicable to a particular Product. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

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

Solicitation means the documents used by the State of Utah, as the Lead State, to obtain Contractor's Proposal.

Statement of Work means a written statement in the solicitation, Participating Addendum or Order that describes the Purchasing Entity's service needs and expectations.

3. Term of the Master Agreement: The initial term of this Master Agreement is for ten (10) years with no renewal options.

4. Amendments: The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the Lead State and Contractor.

5. Assignment/Subcontracts: Contractor shall not assign, sell, transfer, or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State, however, Contractor may use its affiliates and Fulfilment Partners identified in Contractor's proposal to provide the Products and/or Services, provided that Contractor remains responsible for the Products and/or performance of Service.

The Lead State reserves the right to assign contract administration duties to the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint, but the Lead State shall remain a Party to this Master Agreement.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement and an amendment is not necessary.

7. Termination: Unless otherwise stated, this Master Agreement may be terminated by either party upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision shall not affect the rights and obligations attending orders outstanding at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Services delivered and accepted, data ownership, Contractor obligations regarding Purchasing Entity Data, rights attending default in performance an applicable Service Level of Agreement in association with any Order, Contractor obligations under Termination and Suspension of Service, and any responsibilities arising out of a Security Incident or Data Breach. Termination of the Master Agreement due to Contractor default may be immediate.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity's or Purchasing Entity's clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession

without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, may cause irreparable injury to Purchasing Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release of any information that pertains to the potential work or activities covered by the Master Agreement , including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or Participating Addendum shall not be made without prior written approval of the Lead State or a Participating Entity.

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

10. Defaults and Remedies

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

(1) Nonperformance of contractual requirements; or

(2) A material breach of any term or condition of this Master Agreement; or

(3) Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

(4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

(5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and Lead State shall have the right to exercise any or all of the following remedies:

(1) Exercise any remedy provided by law; and

(2) Terminate this Master Agreement and any related Contracts or portions thereof; and

(3) Suspend Contractor from being able to respond to future bid solicitations; and

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

12. Force Majeure: Neither party shall be in default by reason of any failure in performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

13. Indemnification

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, and employees from and against damages finally awarded by a court of competent jurisdiction or otherwise agreed to by Contractor in a written settlement for any death, injury, or damage to tangible property arising directly or indirectly from the negligence or misconduct of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement.

b. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO Value Point, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees ("Indemnified Party") from and against any third party claim that Contractor's Product or Service infringes a patent or copyright enforceable in a country that is a signatory to the Berne Convention and pay the resulting costs and damages finally awarded against the Indemnified Party by a court of competent jurisdiction or the amounts stated in a written settlement negotiated by Contractor, including reasonable attorney's fees. The foregoing obligations are subject to the following: Indemnified Party (a) notifies Contractor promptly in writing of such claim; (b)

grants Contractor sole control over the defense and settlement thereof; (c) reasonably cooperates in response to a Contractor request for assistance; and (d) is not in material breach of this Master Agreement. Should any such Product or Service become, or in Contractor's opinion be likely to become, the subject of such a claim, Contractor may, at its option and expense (1) procure for Indemnified Party the right to make continued use thereof; (2) replace or modify such so that it becomes non-infringing; (3) request return of the Product and, upon receipt thereof, refund the price paid by Indemnified Party, less straight-line depreciation based on a five (5) year useful life for products; or (4) discontinue the Service and refund the portion of any pre-paid Service fee that corresponds to the period of Service discontinuation. Contractor shall have no liability to the extent that the alleged infringement arises out of or relates to: (A) the use or combination of a Product or Service with third party products or services; (B) use for a purpose or in a manner for which the Product or Service was not designed; (C) any modification made by any person other than Contractor or its authorized representatives; (D) any modifications to a Product or Service made by Contractor pursuant to Indemnified Party's specific instructions; (E) any technology owned or licensed by Indemnified Party from third parties; or (F) use of any older version of the Software when use of a new software release made available to Indemnified Party would have avoided the infringement. THIS SECTION STATES INDEMNIFIED PARTY'S SOLE AND EXCLUSIVE REMEDY AND CONTRACTOR'S ENTIRE LIABILITY FOR THIRD PARTY INFRINGEMENT CLAIMS.

c. LIMITATION ON DIRECT DAMAGES. EXCEPT WITH RESPECT TO CLAIMS ARISING UNDER THIS SECTION 13, CONTRACTOR'S TOTAL LIABILITY AND THE INDEMNIFIED PARTY'S SOLE AND EXCLUSIVE REMEDY FOR ANY CLAIM OF ANY TYPE WHATSOEVER ARISING OUT OF PRODUCTS OR SERVICES PROVIDED HEREUNDER, SHALL BE LIMITED TO PROVEN DIRECT DAMAGES CAUSED BY CONTRACTOR'S SOLE NEGLIGENCE IN AN AMOUNT NOT TO EXCEED THREE MILLION U.S. DOLLARS (US$3,000,000). THIS LIMITATION IS CUMULATIVE AND NOT PER INCIDENT.

d. NO INDIRECT DAMAGES. EXCEPT WITH RESPECT TO CLAIMS REGARDING VIOLATION OF CONTRACTOR'S INTELLECTUAL PROPERTY RIGHTS OR CLAIMS ARISING UNDER THIS SECTION 13, NEITHER INDEMNIFIED PARTY NOR CONTRACTOR SHALL HAVE LIABILITY TO THE OTHER FOR LOST OR DAMAGED DATA (EXCEPT FOR A LOSS OF A PARTICIPATING ENTITY'S DATA CAUSED BY CONTRACTOR'S NEGLIGENCE), SPECIAL, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL OR INDIRECT DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUES) EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

e. Regular Back-ups. As part of its obligation to mitigate damages, the indemnified party shall take reasonable data back-up measures. In particular, the indemnified party shall provide for a daily back-up process and back-up the relevant data before Contractor performs any remedial, upgrade or other works on purchasing entity's production systems. To the extent Contractor's liability for loss of data is not anyway excluded under this Master Agreement, Contractor shall in case of data loses only be liable for the typical effort to recover the data which would have accrued if purchasing entity had appropriately backed up its data.

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

15. Individual Customers: Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

16. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed, or admitted, to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum, only after VMware has been unable to provide replacement insurance prior to the effective date of cancellation or non-renewal.

b. Coverage shall be written on an occurrence basis, except Technology Errors & Omissions, Data Breach & Privacy/Cyber Liability and Professional Liability, which may be written on a claims made basis. Crime insurance shall be written on a "Loss Discovered basis". The minimum acceptable limits shall be as indicated below for each of the following categories:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than $1 million per occurrence/$3 million general aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	**Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions** Minimum Insurance Coverage
Low Risk Data	$2,000,000
Moderate Risk Data	$5,000,000
High Risk Data	$10,000,000

(3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

(4) Professional Liability (Technology Errors & Omissions). As applicable, Professional Liability Insurance Policy in the minimum amount of $1,000,000 per occurrence and $1,000,000 in the aggregate, written on a claims made basis that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and Contractor shall make reasonable efforts to provide thirty (30) calendar days prior notice of intended revocation to Purchasing Entity and Participating Entity by the Contractor.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a certificate of insurance or memorandum of insurance that except for workers compensation, Employers' Liability, Errors and Omissions, Data Breach Privacy/Cyber Liability and Employee Dishonesty Insurance (1) provides that the Contractor's liability insurance policy shall be primary, but only to the extent of Contractor's contributory negligence with regard to services performed under this agreement, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a

Participating Addendum, or the Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized or admitted to operate in all states); and a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements). Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

17. Laws and Regulations: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

18. No Waiver of Sovereign Immunity: In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of a Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

19. Ordering

a. Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

b. This Master Agreement permits Purchasing Entities to define project-specific requirements and informally compete the requirement among other firms having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to Purchasing Entity rules and policies. The Purchasing Entity may in its sole discretion determine which firms should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

d. Contractor shall not begin providing Services without a valid Service Level Agreement or other appropriate commitment document compliant with the law of the Purchasing Entity.

e. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

(1) The services or supplies being delivered;
(2) The place and requested time of delivery;
(3) A billing address;
(4) The name, phone number, and address of the Purchasing Entity representative;
(5) The price per unit or other pricing elements consistent with this Master Agreement and the contractor's proposal;
(6) A ceiling amount of the order for services being ordered; and
(7) The Master Agreement identifier and the Participating State contract identifier.

g. All communications concerning administration of Orders placed shall be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality

requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office[3].

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

e. NASPO ValuePoint is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO ValuePoint cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

f. Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor.

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have

[3] Chief Information Officer means the individual designated by the Governor with Executive Branch, enterprise-wide responsibility for the leadership and management of information technology resources of a state.

the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Participating Entities and Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement. This limitation does not prohibit: payments by employees of a Purchasing Entity as explicitly permitted under this agreement; and fees associated with inventory transactions with other governmental or nonprofit entities under cooperative agreements and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

21. Payment: Unless otherwise stipulated in the Participating Addendum, Payment is normally made within 30 days following the date of a correct invoice is received. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of disputed amount of an invoice. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

22. Data Access Controls: Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff") who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor shall not access a Purchasing Entity's user accounts or Data, except on the course of data center operations, response to service or technical issues, as required by the express terms of this Master Agreement, or at a Purchasing Entity's written request.

Contractor may not share a Purchasing Entity's Confidential Information with its parent corporation, other affiliates, or any other third party without the Purchasing Entity's express written consent.

23. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in a manner that is, at all times during the term of this Master Agreement, at a level equal to or more stringent than those specified in the Solicitation.

24. Public Information: This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

25. Purchasing Entity Data: Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

Contractor shall not use any information collected in connection with this Master Agreement, including Purchasing Entity Data, for any purpose other than fulfilling its obligations under this Master Agreement.

26. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

b. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or orders or underpayment of fees found as a result of the examination of the Contractor's records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

d. The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement and applicable Participating Addendum terms. The purchasing entity may perform this audit or contract with a third party at its discretion and at the purchasing entity's expense.

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The

NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

Additionally, some states may require an additional administrative fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee shall be based on the gross amount of all sales at the adjusted prices (if any) in Participating Addenda.

28. System Failure or Damage: In the event of system failure or damage caused by Contractor or its Services, the Contractor agrees to use its reasonable efforts to restore or assist in restoring Contractor's software.

29. Title to Product: Reserved**.**

30. Data Privacy: The Contractor must comply with all applicable laws related to data privacy and security. Prior to entering into a SLA with a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine the Data Categorization to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and Low Risk Data. The Purchasing Entity must document the Data Categorization in the Order. For hosted services, the Purchasing Entity rather than the Contractor will load Purchasing Entity Data into the Products, and the Contractor will not have access to or knowledge of the Data Categorization of such Purchasing Entity Data.

31. Warranty: The Contractor warrants the following:

a. Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Services described in this Master Agreement.

b. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.

c. Contractor represents and warrants that the representations contained in its response to the Solicitation by the Lead State.

d. The Contractor warrants that, to its knowledge, no portion of the Software contains Disabling Code at the time of delivery. The following shall not be deemed Disabling

Code: (1) a feature through the user interface that permits a user to access the Contractor's Web site through a browser over the Internet to access the support and subscription services or to register the Software, or (2) serial numbers that de-activate evaluation copies of the Software after a period of time, making the Software unusable, or (3) code which limits the number of processors upon which the Software will operate, the number of concurrent virtual machines executing, or code which limits any specific virtual machine to a given number of virtual processors.

e. In addition, express warranties pertaining to specific Products and Services will be provided pursuant to the applicable Terms of Service and/or End User License Agreement.

f. THE EXPRESS WARRANTIES SET FORTH IN THIS SECTION AND IN THE APPLICABLE TERMS OF SERVICE AND/OR END USER LICENSE AGREEMENT ATTACHED HEREINTO OR REFERENCED IN AN ORDER, ARE IN LIEU OF ALL OTHER WARRANTIES, AND, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE CONTRACTOR DISCLAIMS, ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE REGARDING OR RELATING TO THE PRODUCTS, SERVICES OR ANY OTHER MATERIALS FURNISHED OR PROVIDED TO A PURCHASING ENTITY. THE CONTRACTOR WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO A PURCHASING ENTITY BY THE CONTRACTOR. NO EMPLOYEE, AGENT, REPRESENTATIVE OR AFFILIATE OF THE CONTRACTOR HAS THE AUTHORITY TO BIND THE CONTRACTOR TO ANY ADDITIONAL REPRESENTATIONS OR WARRANTIES.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement. Any transition services requested by a Purchasing Entity involving knowledge transfer and support will be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, when reasonable, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity's Confidential Information during the transition services and thereafter as required by the Purchasing Entity.

33. Waiver of Breach: Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a

waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

34. Assignment of Antitrust Rights: Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

35. Debarment : The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

36. Performance and Payment Time Frames that Exceed Contract Duration: All maintenance or other agreements for services entered into during the duration of an SLA and whose performance and payment time frames extend beyond the duration of this Master Agreement shall remain in effect for performance and payment purposes (limited to the time frame and services established per each written agreement). No new leases, maintenance or other agreements for services may be executed after the Master Agreement has expired. For the purposes of this section, renewals of maintenance, subscriptions, SaaS subscriptions and agreements, and other service agreements, shall not be considered as "new."

37. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

38. No Guarantee of Service Volumes: The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Services. The Contractor acknowledges and agrees that there is no such representation, warranty or condition.

39. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered into a multi-year agreement with SciQuest, Inc. whereby SciQuest will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provided customers information regarding the Contractors website and ordering information.

At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the customer to have.

40. Contract Provisions for Orders Utilizing Federal Funds: Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have

additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

41. Government Support: No support, facility space, materials, special access, personnel or other obligations on behalf of the states or other Participating Entities, other than payment, are required under the Master Agreement.

42. NASPO ValuePoint Summary and Detailed Usage Reports: In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://www.naspo.org/WNCPO/Calculator.aspx. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (1) state; (2) entity/customer type, e.g. local government, higher education, K12, non-profit; (3) Purchasing Entity name; (4) Purchasing Entity bill-to and ship-to locations; (4) Purchasing Entity and Contractor Purchase Order identifier/number(s); (5) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (6) Purchase Order date; (7) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-Rom, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment F.

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical identifier, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development

Coordinator with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any PA roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due 30 days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

f. If requested by a Participating Entity, the Contractor must provide detailed sales data within the Participating State for Orders placed under this Master Agreement.

43. Entire Agreement: This Master Agreement, along with any exhibits and/or attachment, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum or an Order with a Participating Entity or an Order with a Purchasing Entity. Except as agreed to in this Master Agreement, a Participating Addendum, or Order, no click-through, or other end user terms and conditions or agreements required by the Contractor ("Additional Terms") provided with any Services hereunder shall be binding on Participating Entities or Purchasing Entities, even if use of such Services requires an affirmative "acceptance" of those Additional Terms before access is permitted.

Exhibits:

The Contractor's terms and conditions that have been agreed upon are included in this Master Agreement. The VMware terms and conditions that govern a Purchasing Entity's access to and use of any Product is attached hereto as Exhibit 1 to the Agreement for reference, and the then-current version of such terms and conditions found at http://www.vmware.com/download/eula.html will apply at the time an Order is placed by such Purchasing Entity.

- vCloud Air Terms of Service
- vCloud Air Service Level Agreement
- AirWatch Terms of Service
- AirWatch End User License Agreement
- vRealize Terms of Service
- VMware Horizon Air Terms of Service
- Socialcast Terms of Service
- PSO General Terms and Conditions
- VMware End User License Agreement and Subscription and Support Terms

VMware vCloud® Air™

TERMS OF SERVICE

Last updated: September 15, 2016

By accessing the VMware hosted service specified in your Order (the "**Service Offering**"), you agree to be bound by these terms of service between you and VMware ("**Agreement**"). This Agreement also includes the applicable Service Description, Privacy Addendum, Third Party Terms, Support Policy, and Service Level Agreement. If you do not agree to this Agreement, you must not access the Service Offering. "**You**" means you individually or the entity that you represent. If you are entering into this Agreement for an entity, you represent to us that you have legal authority to bind that entity. "**VMware**," "**we**," or "**us**" means VMware, Inc., a Delaware corporation, to the extent that you purchase the Service Offering in the United States and VMware International Limited, a company organized and existing under the laws of Ireland, to the extent that you purchase the Service Offering elsewhere. Capitalized terms used in this Agreement are defined throughout this Agreement and in Section 14.

1. The Service Offering.

1.1 Generally. This Agreement governs your access to and use of the Service Offering. We may deliver the Service Offering to you with the assistance of our affiliates, licensors and service providers. You will comply with all laws, rules and regulations applicable to your use of the Service Offering. You also will comply with the applicable Third Party Terms, Service Description, Privacy Addendum, and Support Policy. If you access the Service Offering, or any of its features or functionality, on an evaluation or beta basis, please see Section 1.5 for other terms that apply to you.

1.2 Access to the Service Offering. You may access and use the Service Offering solely for your own benefit and only in accordance with this Agreement. To access the Service Offering, you must register for the Service Offering and set up an authorized account with Login Credentials. You may monitor and manage your Service Offering account via the My VMware Portal available at www.vmware.com/accounts and through the Service Offering Portal available at http://vcloud.vmware.com. You must keep confidential your Login Credentials. If you set up an authorized account for an organization, you must require that all authorized Users of that account (including anyone providing services to you) keep confidential their Login Credentials. You must keep your registration information accurate, complete and current for as long as you use the Service Offering. You are responsible for any use that occurs under your Login Credentials, including any activities by you or your employees, contractors or agents. If you believe an unauthorized person has gained access to your Login Credentials, you must notify us as soon as possible by submitting a Severity 1 Service Request (see the applicable Support Policy).

1.3 Verifying Compliance; Cooperation. We have the right to verify your compliance with this Agreement. If we seek to verify that compliance, you will provide information or other materials reasonably requested by us to assist in the verification. We monitor the overall performance and stability of the infrastructure of the Service Offering. You may not block or interfere with that monitoring. If we reasonably believe a problem with the Service Offering may be attributable to Your Content or your use of the Service Offering, you will cooperate with us to identify the source of and resolve that problem.

1.4 Third Party Content. As part of your use of the Service Offering, you may receive access to Third Party Content, which is subject to separate terms. If so, those separate terms will prevail over this Agreement as to your use of the Third Party Content. Third Party Content is available "AS IS" without indemnification, support (unless otherwise noted in the Third Party Terms), or warranty of any kind. You are responsible for reviewing, accepting, and complying with any third party terms of use or other restrictions applicable to the Third Party Content. Those terms will be available to you in the Third Party Terms or through a notification within the Service Offering. We reserve the right to suspend or terminate the Third Party Content at any time. We will use commercially reasonable efforts to provide reasonable notice of that suspension or termination.

1.5 Evaluation and Beta Use. If you access the Service Offering, or a feature or functionality of the Service Offering, on an evaluation or beta basis (either referred to as the "Evaluation Service"), then you may use the Evaluation Service only for evaluation purposes and for the period we specify. Unless we specify otherwise, any use of the Service Offering on an evaluation basis will be for a period of 30 days, beginning on the date we provide you Login Credentials. You must not use the Evaluation Service for any production computing activity. Notwithstanding any other provision of this Agreement, we provide the Evaluation Service (a) free of charge and without support; and (b) "AS IS" without indemnification or warranty of any kind. The Service Level Agreement does not apply to the Evaluation Service. Also, certain features or services described in the Service Description may not be available for the Evaluation Service. You will not have access to the Evaluation Service or to Your Content when it terminates. Any Evaluation Service features and functionality do not constitute an implied commitment to offer them to you or anyone as part of the Service Offering on a generally available basis.

1.6 Open Source Software. You may receive open source software when you use the Service Offering. Any open source software distributed to you is made available under the applicable open source license, which can be found at: http://www.vmware.com/download/open_source.html. You may obtain a copy of these licenses and any source code (and modifications) that we are required to make available under these licenses (the "**Source Files**") at http://www.vmware.com/download/open_source.html or by sending a written request, with your name and address, to: VMware, Inc., 3401 Hillview Avenue, Palo Alto, CA 94304, United States of America. All written requests must clearly specify: Open Source Files Request, Attention: General Counsel. This offer to obtain a copy of the Source Files is valid for three years from the date you last received open source software as part of the Service Offering.

2. Data Protection and Security.

2.1 Data Protection. We will process personal data contained in Your Content, and maintain appropriate technical and organizational measures (administrative, physical and technical safeguards), as set forth in the Privacy Addendum.

2.2 Your Content; Security. You are solely responsible for Your Content. Except as provided by the Privacy Addendum, You are responsible for protecting the security of Your Content, including any access to Your Content that you might provide to your employees, customers or other third parties, and when it is in transit to and from the Service Offering. The Service Offering provides you with certain software and functionality to help you protect Your Content from unauthorized access. You must take and maintain appropriate steps regarding the security, protection and backup of Your Content, which might include the use of encryption technology to protect Your Content from unauthorized access. You are responsible for providing any necessary notices to Users and for obtaining any legally-required consents from Users concerning their use of the Service Offering. You are responsible for complying with any laws or regulations that might apply to Your Content. You are responsible for any losses or other consequences arising from your failure to encrypt or back up Your Content.

3. Acceptable Use.

3.1 General Restrictions. You and any Users accessing the Service Offering through you may not: (a) resell or sublicense the Service Offering; or (b) use or access the Service Offering: (i) in a way prohibited by law, regulation, governmental order or decree; (ii) to violate any rights of others; (iii) to try to gain unauthorized access to, test the vulnerability of, or disrupt the Service Offering or any other service, device, data, account or network; (iv) to spam or distribute malware; (v) in a way that could harm the Service Offering or impair anyone else's use of it; (vi) in a way intended to work around the Service Offering's technical limitations, recurring fees or usage limits; or (vii) in any application or situation where failure of the Service Offering could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage. You must ensure that your Users comply with the terms of this Agreement, and you agree that if you become aware of any violation by one of your Users, you will immediately terminate that User's access to Your Content. If we have reason to believe that you or your Users have breached this Agreement, we or our designated representative may review your use of the Service Offering, including your account, Your Content, and your records, to verify your compliance with this Agreement.

3.2 Content Restrictions. You will take steps to ensure that any User does not post content that: (a) may create a risk of harm, loss, physical or mental injury, emotional distress, death, disability, disfigurement, or physical or mental illness to anyone; (b) may create a risk of any other loss or damage to any person or property; (c) may constitute or contribute to a crime or tort; (d) contains any information or content that is illegal, unlawful, harmful, abusive, pornographic, racially or ethnically offensive, defamatory, infringing, invasive of personal privacy or publicity rights, harassing, humiliating to other people (publicly or otherwise), libelous, threatening, or otherwise objectionable; or (e) contains any information or content that you do not have a right to make available under any law or under contractual or fiduciary relationships. You are responsible for any software, product or service that a third party licenses, sells or makes available to you that you install or use with the Service Offering. Your use of that software, product or service is governed by separate terms between you and that third party. We are not a party to and are not bound by any of those separate terms. You represent and warrant that Your Content does not and will not violate any third-party rights, including any Intellectual Property Rights, and rights of publicity and privacy. You will ensure that your use of the Service Offering complies at all times with your privacy policies and all applicable laws and regulations, including any encryption requirements.

3.3 Violations of Acceptable Use. If you become aware that any of Your Content or any User's access to or use of Your Content violates Sections 3.1 or 3.2, you will take immediate action to remove the applicable part of Your Content or suspend the User's access. We may also ask you to take action within a certain time period, and if you fail to comply with the request, we may suspend your account pursuant to Section 6.

3.4 Notification of Infringement Concerns. If you believe that your copyrighted work has been copied and is accessible on the Service Offering in a way that constitutes copyright infringement, please send a notice to our copyright agent providing the following information: (1) a description of the copyrighted work that you claim has been infringed and a description of the infringing activity, (2) a description of the location of the material that you claim is infringing is located, such as the URL where it is posted, (3) your name, address, telephone number and email address, (4) a statement by you that you have a good faith belief that the disputed use of the material is not authorized by the copyright owner, its agent or the law (5) a statement made by you, under penalty of perjury, that the above information in your notice of infringement concerns is accurate and that you are the copyright owner or are authorized to act on the copyright owner's behalf, and (6) your electronic or physical signature, as the copyright owner or as the person authorized to act on the owner's behalf. VMware's copyright agent for notice of claims of copyright infringement can be reached as follows. Solely for purposes of reporting copyright infringement, please contact VMware's copyright agent:

VMware, Inc.
Intellectual Property Counsel

3401 Hillview Avenue
Palo Alto, California, 94304
United States of America.
Email: copyright@vmware.com
Tel: 877-486-9273

4. IP Ownership.

4.1 Ownership of Service Offering. We and our licensors own and retain all right, title and interest in and to the Service Offering and any related VMware Software, including all improvements, enhancements, modifications and derivative works thereof, and all Intellectual Property Rights therein. This includes any information that we collect and analyze in connection with the Service Offering, such as usage patterns, user feedback and other information to improve and evolve our software products and services offerings. Your rights to use the Service Offering are limited to those expressly granted in this Agreement. No other rights with respect to the Service Offering, any related VMware Software, or any related Intellectual Property Rights are implied.

4.2 Ownership of Your Content. You and your authorized Users retain all right, title and interest in and to Your Content and all Intellectual Property Rights therein. Our rights to access and use Your Content are

limited to those expressly granted in this Agreement. No other rights with respect to Your Content or any related Intellectual Property Rights are implied.

4.3. Feedback. We will be free to use for any purpose any feedback (such as comments or suggestions) that you provide to us regarding the Service Offering. You hereby grant to us a non-exclusive, perpetual, irrevocable, royalty-free, transferable, worldwide right and license, with the right to sublicense, to use, reproduce, perform, display, disclose, distribute, modify, prepare derivative works of and otherwise exploit the feedback without restriction in any manner now known or in the future conceived and to make, use, sell, offer to sell, import and export any product or service that incorporates the feedback.

5. Orders, Delivery, Payment, and Taxes.

5.1 Orders Generally. All Orders issued to VMware are subject to the terms of this Agreement and are not binding until accepted by VMware. We are not required to provide any Service Offering to you until you provide all information we require for processing your Order. Your Order will be deemed accepted when we authorize the purchased Service Offering for your Login Credentials.

5.2 Delivery. When VMware accepts your Order for the Service Offering, we will deliver the corresponding Login Credentials to you by email to the address associated with your account. If VMware ships a physical object in connection with an add-on feature of the Service Offering, shipping and delivery terms are Ex Works VMware's regional fulfillment facility (INCOTERMS 2010).

5.3 Direct Orders. This Section 5.3 applies only to Orders and purchases you make directly with VMware. A VMware authorized reseller might specify similar terms when you make an Order or purchase through that reseller.

5.3.1 Purchase Orders. For Subscription-based Service Offering orders placed directly with VMware, you must issue a purchase order to VMware for the initial Service Offering order, but a purchase order is not required for us to invoice you for the monthly billings that occur after the initial Order billing.

5.3.2 Invoicing and Payment. We will bill you as specified in the Service Description. You will pay all fees for use of the Service Offering in the amount and currency specified in your invoice by one of the payment methods that we support as specified in the Service Description, and in any event no later than 30 days after the date of the invoice. For an OnDemand-based Service Offering, you will pay in arrears on a monthly basis the applicable fees based on your actual metered usage of the Service Offering. For a Subscription-based Service Offering, you will pay in advance the applicable fees for the monthly or prepaid charges due, and you will pay in arrears the initial monthly fees and for any metered usage components consumed. The applicable fees for the Service Offering will be governed by the then-current applicable price list at the time of invoicing. We may increase or add new fees for the Service Offering by notifying you at least 30 days in advance.

5.3.3 Taxes. Service Offering fees are exclusive of Taxes. "**Taxes**" means any sales, VAT, GST (Goods and Services Tax), use, gross receipts, business and occupation, and other taxes (other than taxes on our income), export and import fees, customs duties and similar charges imposed by any government or other authority. You shall pay or reimburse us for all Taxes arising out of the transactions contemplated by this Agreement. If you are required to pay or withhold any Tax for payments due under this Agreement, you shall gross up your payments to us so that we receive sums due in full and free of any deductions. If you are required to pay any Tax to a taxing authority, you will also provide documentation to us showing that you paid those Taxes to the relevant taxing authority. You hereby confirm that we can rely on the name and address you provide to us when you agree to the Service Offering or in connection with your payment method as being the place of supply for sales tax and income tax purposes or as being the place of supply for VAT purposes where you have established your business.

6. Temporary Suspension.

6.1 Generally. We may suspend your use of the Service Offering if we reasonably determine: (a) payment for the Service Offering is not received within 30 days from the date on which payment is due; (b) you are, or your use of the Service Offering is, in breach of this Agreement; (c) you fail to address our request to take action as specified in Section 3.3; (d) your use of the Service Offering poses a security risk to the Service Offering or other users of the Service Offering; or (e) suspension is required pursuant to our receipt of a

subpoena, court order, or other request by a law enforcement agency. We will give you notice before we suspend, **subject to** applicable law, **and unless** we reasonably determine that **providing the notice presents** risk of harm to the Service Offering or any person or property.

6.2 Effect of Suspension. You will remain responsible for all fees incurred before or during any suspension. You will not be entitled to any service credits under any applicable Service Level Agreement that you might have otherwise accrued during the period of suspension.

7. Term and Termination.

7.1 Term of Agreement. This Agreement will be in effect until it is terminated as permitted herein or under the Service Description. For Subscription-based Service Offerings, the subscription will automatically renew as specified in the Service Description, unless terminated as permitted therein.

7.2 Termination for Cause. We may terminate this Agreement effective immediately upon sending you an email notice if you: (a) breach any provision of Sections 3.1 or 3.2; (b) do not resolve the underlying cause resulting in a suspension of your account pursuant to Section 6.1 (other than suspension due to a subpoena, court order, or other request by a law enforcement agency) within 10 days after your account is suspended; (c) commit a material breach of this Agreement that cannot be cured; or (d) terminate or suspend your business.

7.3 Termination for Insolvency. We may terminate this Agreement effective immediately upon sending you an email notice if you: (a) become insolvent, admit in writing your inability to pay your debts as they mature, or make an assignment for the benefit of creditors; or (b) become subject to control of a trustee, receiver or similar authority or any bankruptcy or insolvency proceeding.

7.4 Effect of Termination. Upon the effective date of termination of this Agreement for any reason: (a) all rights granted to you under this Agreement, including your ability to access the Service Offering, will immediately terminate; and (b) you must promptly discontinue all use of the Service Offering and delete or destroy any of our Confidential Information. Deletion and retrieval of Your Content will be handled as set forth in the Privacy Addendum. Section 1.6 (Open Source Software), 3 (Acceptable Use), 4 (IP Ownership), 5 (Orders, Delivery, Payment and Taxes), 7 (Term and Termination), 9 (Disclaimer), 11 (Limitation of Liability), 12 (Confidential Information), 13 (General), 14 (Definitions), 15 (Provisions for Specific Data Centers), and the Privacy Addendum will survive the termination of this Agreement. Termination of your use of the Service Offering (except to the extent that the termination is permitted under Sections 10.3 and 13.3 of this Agreement or Section 3.6 of the Service Description) will not entitle you to any refunds, credits, or exchanges, and you will be liable for all usage and other fees incurred up to the termination effective date, including any monthly billing fees for the remaining term of a Subscription-based Service Offering after the termination effective date.

8. Support and Subscription Services. When applicable, and subject to the terms of this Agreement, we will provide support for the Service Offering in accordance with the terms specified in the applicable Support Policy. We will not provide support to any end users of Your Content.

9. Disclaimer. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, WE AND OUR LICENSORS AND SERVICE PROVIDERS DISCLAIM ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, SATSIFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE, RELATING TO THE SERVICE OFFERING OR ANY MATERIALS OR SERVICES PROVIDED TO YOU UNDER THIS AGREEMENT. WE AND OUR LICENSORS AND SERVICE PROVIDERS DO NOT WARRANT THAT THE SERVICE OFFERING WILL BE UNINTERRUPTED OR FREE FROM DEFECTS, OR THAT THE SERVICE OFFERING WILL MEET (OR IS DESIGNED TO MEET) YOUR BUSINESS REQUIREMENTS.

10. Indemnification.

10.1 Indemnification by You. You will defend and indemnify us against any third party claim arising from or relating to: (a) Your Content; (b) any infringement or misappropriation of any Intellectual Property Rights by you, Users or your suppliers in connection with your use of the Service Offering; (c) any violation of law by you or Users in connection with use of the Service Offering; (d) your or Users' use of the Service Offering in violation of this Agreement, or (e) your or Users' use of any Third Party Content. We will (1) provide you with

notice of the claim within a reasonable period of time after learning of the claim; and (2) reasonably cooperate in response to your requests for assistance. You may not settle or compromise any indemnified claim without our prior written consent.

10.2 Defense and Indemnification. Subject to the remainder of this Section 10, we will defend you against an Infringement Claim and indemnify you from the resulting costs and damages finally awarded against you to that third party by a court of competent jurisdiction or agreed to in settlement. You will (a) provide us with notice of any Infringement Claim within a reasonable period of time after learning of it; (b) allow us sole control over the claim's defense and settlement; and (c) reasonably cooperate in response to our requests for assistance. You may not settle or compromise any Infringement Claim without our prior written consent.

10.3 Remedies. If the Service Offering becomes, or in our opinion is likely to become, the subject of an Infringement Claim, we will at our option and expense: (a) procure the rights necessary for you to keep using the Service Offering; (b) modify or replace the Service Offering to make it non-infringing; or (c) terminate this Agreement and refund any pre-paid fees for a Subscription-based Service Offering pro-rated for its remaining term.

10.4 Exclusions. We will have no obligation under this Section 10 or otherwise with respect to any claim based on: (a) a combination of VMware Software with non-VMware products or content, including Your Content; (b) use of the Service Offering for a purpose or in a manner not specified in this Agreement or the Service Description; (c) any modification to the Service Offering made without our express written approval; or (d) any Service Offering provided on a no-charge basis, including an Evaluation Service as described in Section 1.5. This Section 10 states your exclusive remedy for any infringement claims.

11. Limitation of Liability.

11.1 Generally. TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT WILL WE BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE OF THE SERVICE OFFERING OR YOUR CONTENT, LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY OR OTHERWISE. IN ANY EVENT, OUR LIABILITY UNDER THIS AGREEMENT WILL NOT, REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE, EXCEED THE GREATER OF: (A) THE AGGREGATE FEES PAID OR PAYABLE TO US FOR YOUR ACCESS TO AND USE OF THE SERVICE OFFERING IN THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO THE CLAIM, OR (B) FIVE THOUSAND U.S. DOLLARS ($5,000 USD) (OR THE EQUIVALENT IN LOCAL CURRENCY), REGARDLESS OF WHETHER WE OR OUR LICENSORS OR SERVICE PROVIDERS HAVE BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE. THE LIMITATIONS OF LIABILITY IN THIS SECTION 11.1 WILL NOT APPLY TO (A) VMWARE'S INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT OR (B) ANY LIABILITY WHICH MAY NOT BE EXCLUDED BY APPLICABLE LAW.

11.2 Further Limitations. Our licensors and service providers will have no liability of any kind under this Agreement. You may not bring a claim under this Agreement more than eighteen (18) months after the cause of action arises.

12. Confidential Information.

12.1 Protection. A party may use Confidential Information of the other party solely to exercise its rights and perform its obligations under this Agreement or as otherwise permitted under this Agreement. Each party will disclose the Confidential Information of the other party only to the employees, service providers or contractors of the recipient party who have a need to know the Confidential Information for purposes of this Agreement and who are under a duty of confidentiality no less restrictive than each party's duty under this Agreement. Each party will use reasonable care to protect the confidentiality of the other party's Confidential Information.

12.2 Exceptions. The recipient's obligations under Section 12.1 with respect to any Confidential Information will terminate if the recipient can show by written records that the information: (a) was already rightfully known to the recipient at the time of disclosure by the other party; (b) was disclosed to the recipient by a third party

who had the right to make the disclosure without any confidentiality restrictions; (c) is, or through no fault of the recipient has become, generally available to the public; or (d) was independently developed by the recipient without access to, or use of, discloser's Confidential Information. The recipient may disclose Confidential Information to the extent the disclosure is required by law or regulation or the listing rules of any stock exchange. The recipient will provide the other party notice, when practicable, and will take reasonable steps to contest and limit the scope of any required disclosure.

13. General.

13.1 Assignment. You may not assign or transfer this Agreement, in whole or in part, by operation of law or otherwise, without our prior written consent. Any attempted assignment or transfer without that consent will be void. Subject to these limits, this Agreement will bind and inure to the benefit of the parties and their respective successors and assigns.

13.2 Notices. Any notice delivered by us to you under this Agreement will be delivered by email to the email address associated with your account or by posting on either the Service Offering Portal or the My VMware Portal, except as otherwise set forth in this Agreement. You will direct legal notices or other correspondence to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America, Attention: Legal Department.

13.3 Modifications. We may change periodically the Service Offering, the terms of your access to the Service Offering, this Agreement, the Service Description, the Privacy Addendum, the Third Party Terms, the Service Level Agreement, or the Support Policy. It is your responsibility to regularly check the Service Offering and My VMware portals for updates. We will notify you of any material, detrimental change to this Agreement, the Service Description, the Privacy Addendum, the Service Level Agreement, or the Support Policy. In the case of a material, detrimental change to the Service Level Agreement, we will notify you at least 90 days prior to the effective date of the change. The modified Agreement, Service Description, Privacy Addendum, Service Level Agreement, or Support Policy, as applicable, will become effective as of the date stated in that notification. If we make a material, detrimental change to the Service Offering (other than the termination or modification of any beta feature or functionality), this Agreement, the Service Description, the Privacy Addendum, the Service Level Agreement, or the Support Policy, then you may terminate this Agreement no later than 30 days after the effective date of the change. If you terminate this Agreement pursuant to this Section 13.3, the termination will be effective as of the date we receive your notification, unless you state in your notification an effective date that is later but within 45 days after we receive your notification. If you terminate a Subscription-based Service Offering, we will refund any prepaid fees, pro-rated for the remainder of the term, and less any discounts that would not be earned as of the effective date of the termination. Your continued use of the Service Offering after the effective date of any modification to the Agreement, the Service Description, the Privacy Addendum, the Third Party Terms, the Service Level Agreement, or the Support Policy will be deemed acceptance of the modified terms, as applicable.

13.4 Waiver. The waiver of a breach of any provision of this Agreement will not constitute a waiver of any other provision or any later breach.

13.5 Severability. If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions of this Agreement will remain in force.

13.6 Compliance with Laws; Export Control. Each party will comply with all laws applicable to the actions contemplated by this Agreement. You acknowledge that the Service Offering is of United States origin, is provided subject to the U.S. Export Administration Regulations (including "deemed export" and "deemed re-export" regulations), and may be subject to the export control laws of the applicable country. You represent and warrant that (a) you are not, and are not acting on behalf of, (1) any person who is a citizen, national, or resident of, or who is controlled by, the government of any country to which the United States has prohibited export transactions; (2) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List, or any similar designated persons list published for the jurisdiction in which the data center you choose for the Service Offering is located; (b) you will not permit the Service Offering to be used for any purposes prohibited by law, including any prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons; (c) Your Content will not be classified or listed on the United States

Munitions list or similar list published for the jurisdiction in which the data center you choose for the Service Offering is located, or contain defense articles, defense services or ITAR-related data; (d) Your Content will not require an export license and is not restricted under applicable export control laws from export to any country where VMware or VMware's service providers maintain facilities or personnel; and (e) you are not subject, either directly or indirectly, to any order issued by any agency of the United States government, revoking or denying, in whole or in part, your United States export privileges. You will notify VMware immediately if you become subject to any such order.

13.7 Government Regulations. For purposes of sales to government entities in the U.S.: The Service Offering and its documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFARS Section 227.7202 and FAR Paragraph 12.212(b), as applicable. Any use, modification, reproduction, release, performing, displaying or disclosing of the Service Offering and documentation by or on behalf of the U.S. Government will be governed solely by the terms and conditions of this Agreement.

13.8 Force Majeure. We will not be liable for any delay or failure to perform any obligations under this Agreement due to any cause beyond our reasonable control, including acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications or other utility failures, earthquakes, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism or war.

13.9 Construction. The headings of sections of this Agreement are for convenience and are not for use in interpreting this Agreement. As used in this Agreement, the word 'including' means "including but not limited to."

13.10 Governing Law. This Agreement is governed by the laws of the State of California, United States of America (excluding its conflict of law rules), except as follows: for Service Offering purchases where you choose a data center that is outside the United States of America, the governing laws are those of the country in which the data center is located (excluding its conflict of law rules). The United Nations Convention for the International Sale of Goods does not apply. This Agreement does not affect your statutory rights that cannot be waived or changed by contract.

13.11 Third Party Rights. Other than as expressly provided in this Agreement, this Agreement does not create any rights for any person who is not a party to it, and no person who is not a party to this Agreement may enforce any of its terms or rely on any exclusion or limitation contained in it.

13.12 Order of Precedence. The terms of this Agreement will supersede and control over any conflicting or additional terms and conditions of any other purchasing related document issued by you.

13.13 Entire Agreement. This Agreement, as it may be revised by us, is the entire agreement of the parties regarding its subject matter. This Agreement supersedes all prior or contemporaneous communications, understandings and agreements, whether written or oral, between the parties regarding its subject matter.

14. Definitions.

14.1 "**Confidential Information**" means non-public technical, business or other information or materials disclosed or otherwise made available by one party in connection with the Service Offering that are in tangible form and labeled "confidential" or the like, or are provided under circumstances reasonably indicating their confidentiality. Our Confidential Information includes: (1) Login Credentials; and (2) any information or materials relating to the Service Offering. Your Confidential Information does not include Your Content.

14.2 "**Infringement Claim**" means any third party claim that any VMware Software used to provide the Service Offering infringes any patent, trademark or copyright of the third party, or misappropriates a trade secret (but only to the extent that the misappropriation is not a result of your actions) under the laws of: (a) the United States; (b) Canada; (c) the European Economic Area member states; (d) Australia; (e) New Zealand; (f) Japan; or (g) the People's Republic of China, to the extent that those countries are part of your places of use of the Service Offering.

14.3 "**Intellectual Property Rights**" means all worldwide intellectual property rights, including copyrights, trademarks, service marks, trade secrets, patents, patent applications, and moral rights, whether registered or unregistered.

14.4 "**Login Credentials**" mean any passwords, authentication keys or security credentials that enable your access to and management of the Service Offering.

14.5 "**OnDemand-based Service Offering**" means a Service Offering for which you pay for actual usage in arrears on a periodic basis, as specified in your Order.

14.6 "**Order**" means the internet order page, or other ordering document, that specifies your purchase of the Service Offering.

14.7 "**Privacy Addendum**" means the then-current version of the Service Offering Data Privacy Addendum document available at https://www.vmware.com/support/vcloud-air/data-privacy-addendum.html.

14.8 "**Service Description**" means the then-current version of the Service Offering Service Description document available at http://www.vmware.com/files/pdf/vcloud-air/vcloud-air-Service-Description.pdf, which contains technical and other information.

14.9 "**Service Level Agreement**" means the then-current version of the Service Offering Service Level Agreement document available at https://www.vmware.com/support/vcloud-air/sla.

14.10 "**Subscription-based Service Offering"** means a Service Offering for which you pay in advance for use of the Service Offering for a fixed period as specified in your Order. A Subscription-based Service Offering may also include optional services (e.g., add-ons) and metered usage components.

14.11 "**Support Policy**" means the then-current version of the applicable Service Offering Support Policy document available as follows: for the OnDemand-based Service Offering, https://www.vmware.com/support/services/ondemand-online-support.html or https://www.vmware.com/support/services/ondemand-production-support-offerings.html, and for the Subscription-based Service Offering, https://www.vmware.com/support/services/iaas-production.html.

14.12 "**Third Party Content"** means third party data, service, content, software or applications, including open source software.

14.13 "**Third Party Terms**" means the then-current version of the third party terms applicable to Third Party Content that you obtain in connection with the Service Offering that are available at http://www.vmware.com/files/pdf/vcloud-air/vmware-vcloud-air-third-party-terms.pdf.

14.14 "**User**" means any person that accesses Your Content or uses the Service Offering under your Login Credentials.

14.15 "**VMware Software**" means the software programs listed in our commercial price list.

14.16 "**Your Content**" means any and all applications, services, files, information, data or other content uploaded to or published or displayed through the Service Offering by you, Users, or us (acting upon your instructions as part of a service).

15. Provisions for Specific Data Centers. For Service Offering purchases where you choose a data center located in the countries listed below, the following provisions replace or supplement the referenced sections of this Agreement, as noted.

15.1 Australian Data Center:

15.1.1 Supplement Section 9 titled "Disclaimer" with the following additional paragraph:

"Nothing in this Agreement (including this Section 9 and Section 1.5) excludes, restricts or modifies any consumer guarantee, right or remedy conferred on you by the Australian Consumer Law or any other applicable law that cannot be excluded, restricted or modified by agreement. Subject to the preceding sentence, any condition, warranty, guarantee, right or liability which would otherwise be implied in this Agreement or imposed by law is excluded. VMware's liability for any breach of any consumer guarantee, right or remedy conferred by the Australian Consumer Law which cannot be excluded is limited, at VMware's option, to supplying the applicable service again, or paying to have that service provided again."

15.1.2 Replace the first sentence of Section 13.10 titled "Governing Law" with the following:

"This Agreement is governed by the laws of New South Wales, Australia, without regard to conflict of law principles."

15.2 German Data Center:

15.2.1 Replace the last sentence of Section 1.4 titled "Additional Terms; Third Party Content" with the following sentence:

"Except as permitted under Sections 6 and 7, we will only suspend or terminate Third Party Content during a subscription term with thirty (30) days prior notice, in which case we will provide a pro-rata refund of any pre-payments (if any) made for such suspended or terminated Third Party Content."

15.2.2 In Section 1.5 titled "Evaluation and Beta Use", remove the period at the end of the third sentence which reads "[…] (b) "AS IS" without indemnification or warranty of any kind." And add the following to the end of the third sentence:

", except insofar as defects have been fraudulently concealed by us."

15.2.3 Replace Section 7.3 titled "Termination for Insolvency" with the following:

"**7.3** [Reserved]"

15.2.4 Replace Section 9 titled "Disclaimer" with the following:

"**9. Limited Warranty.**

9.1 Qualities. During the Service Offering term, the Service Offering will substantially conform to the applicable Service Description unless otherwise stated herein. We do not commit that the Service Offering will be uninterrupted or that the Service Offering does fulfill any merchantability or fitness for a particular purpose, or will meet (or is designed to meet) your business requirements, unless stated otherwise in the applicable Service Description or individually agreed between the parties.

9.2 Warranty. We will correct any defect in the aforementioned qualities of the Service Offering reported to us by you in writing. If we are unable to correct the defect, we will refund an appropriate portion of the fees paid by you with respect to the affected portion of the affected Service Offering.

9.3 Any Service Credits (as set forth in the Service Level Agreement), will be set off against any refund for breach of warranty, if and to the extent such Service Credits are provided for the same event that entitles you to a refund for breach of warranty.

9.4 Subject to Section 11, the remedies in Section 9.2 are your sole and exclusive remedies for breach of warranty and our sole and exclusive liability for breach of warranty."

15.2.5 Replace Section 11 titled "Limitation of Liability" with the following:

"**11.1 Limitation.** Our liability for a claim of any nature arising out of this Agreement, regardless of whether the claim is based in contract, tort, strict liability, or otherwise,

11.1.1 will be limited to damages that are foreseeable and typical for this type of contract ("vertragstypische und vorhersehbare Schäden") arising from a slight negligent breach of a material contractual obligation ("Kardinalpflicht", i.e. an obligation the fulfillment of which is essential to enable the proper performance of the contract, and on which fulfillment you may rely on); and

11.1.2 will not exceed per damage event (i) EUR 250.000 (Two Hundred Fifty Thousand Euro), or (ii) if the aggregate fees paid or payable to us for your access to and use of the Service Offering in the twelve (12) months prior to the event giving rise to your claim are higher, then those fees for the specific Service Offering given rise to such claim (subject to the limit set forth in Section 11.1.3 below).

11.1.3 In no event will our total and cumulative liability for all claims arising out of this Agreement exceed EUR 500.000 (Five Hundred Thousand Euro).

11.2 Disclaimer of Liability. In case of slight negligence, we will not be liable for any indirect or consequential damages (including, but not limited to any loss of profits, business opportunity, revenue or goodwill), even if we have been advised as to the possibility of such damages.

11.3 Further Limitations. Our licensors and service providers will have no liability of any kind under this Agreement. You may not bring a claim under this Agreement more than eighteen (18) months after the cause of action arises.

11.4 Exceptions. Nothing in this Agreement will limit or exclude our liability for death or personal injury, for intentional act or gross negligence, fraudulent misrepresentation, fraudulent concealment of a defect, mandatory liability under the German Product Liability Act (Produkthaftungsgesetz), or liability for any damages resulting from a breach of a given guarantee."

15.3 United Kingdom Data Center:

15.3.1 Replace the last sentence in Section 1.4 titled "Additional Terms; Third Party Content" with the following sentence:

"Except as permitted under Sections 6 and 7, we will only suspend or terminate Third Party Content during a subscription term with thirty (30) days prior notice, in which case we will provide a pro-rata refund of any pre-payments (if any) made for such suspended or terminated Third Party Content."

15.3.2 Supplement Section 7.3 titled "Termination for Insolvency" with the following:

"(c) if you are deemed unable to pay your debts within the meaning of Section 123 of the Insolvency Act of 1986; or (d) suffer or undergo any similar or analogous suspension or proceeding in any jurisdiction."

15.3.3 Replace the last sentence of Section 10.4 "[Indemnification] Exclusions" with the following:

"This Section 10 states your exclusive remedy for any infringement claims or any assertions or actions arising out of or related to any infringement claims."

15.3.4 Replace the last sentence of Section 11.1 titled "Generally" with the following:

"THE LIMITATIONS OF LIABILITY IN THIS SECTION 11.1 WILL NOT APPLY TO VMWARE'S INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT. NOTHING IN THIS AGREEMENT SHALL LIMIT OR EXCLUDE ANY PARTY'S LIABILITY FOR DEATH OR PERSONAL INJURY, FOR FRAUDULENT MISREPRESENTATION, OR FOR ANY OTHER LIABILITY WHICH MAY NOT BE LIMITED OR EXCLUDED BY APPLICABLE LAW."

15.3.5 Supplement Section 12.2 titled "[Confidential Information] Exceptions" with the following:

"Breach of this Section 12 by the recipient party may cause the disclosing party substantial harm for which monetary damages are an insufficient remedy. Accordingly, each party agrees that the other party may apply for injunctive relief in respect of any threatened or actual breach of this Section 12."

15.3.6 Any reference to "warranty" is deemed to refer to "warranty, condition or other terms" and any reference to "warranties" is deemed to refer to "warranties, conditions or other terms."

(/)

vCloud Air

SUPPORT CENTER

Service Level Agreement for VMware vCloud Air

Last updated: August 31, 2015

This Service Level Agreement ("SLA") is subject to the terms of the applicable Terms of Service for the VMware vCloud Air Service Offerings listed below. Capitalized terms not defined in this SLA will have the meanings specified in the Terms of Service. We reserve the right to change the terms of this SLA in accordance with the Terms of Service for the Service Offering. Prior versions of this SLA are available at https://www.vmware.com/support/vcloud-air/sla_history.html (/support/vcloud-air/sla_history.html).

VMware will use commercially reasonable efforts to ensure that each class of service purchased for an identified user of an instance of a Service Offering ("you" or "Customer") is "Available" during a given calendar month equal to the "Availability Commitment" provided in the table below.

Class of Service	Availability Commitment
Dedicated Cloud	99.99%
Virtual Private Cloud	99.95%
Data Protection	99.95%
Disaster Recovery	99.95%
Virtual Private Cloud OnDemand	99.95%
Object Storage powered by Google Cloud Platform (Standard)	99.9%
Object Storage powered by Google Cloud Platform (Durable Reduced Availability)	99.0%
Object Storage powered by Google Cloud Platform (Nearline Storage)	99.0%

Related Resources

- Terms of Service (/support/vcloud-air/terms-of-service.html)
- Data Privacy Addendum (/support/vcloud-air/data-privacy-addendum.html)
- Service Level Agreement (/support/vcloud-air/sla.html)

Search

Service Description (/content/dam/digitalmarketing/vmware/en/pdf/product/vcloud-air/vcloud-air-service-description.pdf)

- Third Party Terms (/content/dam/digitalmarketing/vmware/en/pdf/vcloud-air/vmware-vcloud-air-third-party-terms.pdf)
- OnDemand Online Support Policy (/support/services/ondemand-online-support.html)
- OnDemand Production Support Policy (/support/services/ondemand-production-support-offerings.html)
- IaaS Production Support Policy (/support/services/iaas-production.html)

If the Availability of a class of service that you purchase is less than the associated Availability Commitment, then you may request Service Credits for that affected class of service. Availability in a given month is calculated according to the following formula:

"Availability" = ((total minutes in a calendar month – total minutes Unavailable) / total minutes in a calendar month) x 100

Unavailability and SLA Events

A class of service will be considered "Unavailable," subject to the Service Level Agreement Limitations set forth below, if VMware's monitoring tools determine one of the following events has occurred ("SLA Event"). The total minutes that a class of service is Unavailable for a particular SLA Event is measured from the time that VMware validates the SLA Event has occurred, as defined below, until the time that VMware resolves the SLA Event such that the Service Offering is Available to you. If two or more SLA Event occurs simultaneously, the SLA Event with the longest duration will be used to determine the total minutes Unavailable.

- Each of the following will be considered an SLA Event for the Dedicated Cloud, Virtual Private Cloud, or Virtual Private Cloud OnDemand Services:
  a) Any of the network interfaces of the Service Offering Network are unavailable for more than three (3) consecutive minutes. The "Service Offering Network" means the network that extends from the network interfaces of physical host servers for a class of service to the outside network interfaces providing the Service Offering's public internet connectivity.
  b) The data store(s) associated with your block level storage for a class of service are unavailable for more than three (3) consecutive minutes.
  c) The self-service console, available at https://vchs.vmware.com (https://vchs.vmware.com), cannot successfully authenticate a simulated user for more than five (5) consecutive minutes.
  d) Your running virtual machines for a class of service become inaccessible for more than five (5) consecutive minutes due to physical host server failures.
- Each of the following will be considered an SLA Event for the Data Protection Service:
  a) The backup storage repository associated with your Data Protection service is unavailable for more than three (3) consecutive minutes.
  b) The start time associated with your backup scheduling window is missed for longer than thirty (30) consecutive minutes.
  c) The standard 24-hour recovery point objective (RPO) is missed for any virtual machines actively enrolled in the service.
  d) Any restore operation for a virtual machine fails to complete due to backup infrastructure failures.
- Each of the following will be considered an SLA Event for the Disaster Recovery Service:
  a) Any of the network interfaces of the Service Offering Network are unavailable for more than three (3) consecutive minutes.
  b) The data store(s) associated with your block level storage for replication is unavailable for more than three (3) consecutive minutes.
  c) The self-service console, available at https://vchs.vmware.com, cannot successfully authenticate a simulated user for more than five (5) consecutive minutes.
  d) Your failed-over virtual machines for a class of service become inaccessible for more than five (5) consecutive minutes due to physical host server failures.
  e) Any built-in service functions for failover testing, planned migration, or live failover and recovery result in virtual machine replicas not powering on in less than 4 consecutive hours from the time a request is acknowledged and approved by VMware.
- The following will be considered an SLA Event for the Object Storage service:
  a) A more than five (5) percent Error Rate for more than ten (10) consecutive minutes – where "Error Rate" means the number of valid requests that result in a response with HTTP Status 500 and Code "Internal Error" divided by the total number of valid requests during each five-minute period.

Service Credits

- For All Classes of Service (except all Object Storage Classes of Service):

  "Service Credits" means an SLA Credit, a Chronic SLA Credit or a Repetitive SLA Credit.

Search

If the Availability of a class of service that you purchase is less than the associated Availability Commitment in a given calendar month, then

Attachment A, Exhibit 1

you may request one (1) SLA Credit, and one (1) additional SLA Credit for each additional 300 minutes the class of service was Unavailable, up to a total of three (3) SLA Credits in a given calendar month. An "SLA Credit" is an amount equal to 10% of the monthly Service Offering recurring or metered (as applicable) subscription charges invoiced by VMware for the affected class of service in the calendar month for which the SLA Credit is due.

If a particular class of service is Unavailable for 24 consecutive hours, then you may request a Chronic SLA Credit. A "Chronic SLA Credit" is an amount equal to 100% of the monthly Service Offering recurring or metered (as applicable) subscription charges invoiced by VMware, for the affected class of service, in the calendar month in which the SLA Credit is due. Any Chronic SLA Credit is in lieu of any SLA Credits that might be otherwise due.

If you are eligible to receive an SLA Credit or a Chronic SLA Credit in three (3) consecutive calendar months and all the credits are related to the same SLA Event type, then you may request a Repetitive SLA Credit. A "Repetitive SLA Credit" is an amount equal 100% of the largest monthly Service Offering recurring or metered (as applicable) subscription charges invoiced by VMware for the affected class of service, in one of the calendar months in which the SLA Event occurred. If an SLA Credit or a Chronic SLA Credit was already received in the Repetitive SLA Credit period, then the amount of the Service Credit that you may request will be the difference between the aggregate amount of Service Credits received and the Repetitive SLA Credit.

- For Object Storage Classes of Service:

  For all Object Storage classes of service, "Service Credits" means a First SLA Credit or a Second SLA Credit.

  For Object Storage powered by Google Cloud Platform (Standard):

  - If the Availability of this class of service is less than the associated Availability Commitment, but does not exceed Unavailability of more than 438 minutes total, in a given calendar month, then you may request one (1) First SLA Credit. For this class of service, a "First SLA Credit" is an amount equal to 10% of the monthly Service Offering recurring or metered (as applicable) subscription charges invoiced by VMware in the calendar month for which the SLA Credit is due.
  - If this class of service is Unavailable for more than 438 minutes total in a given calendar month, then you may request a Second SLA Credit. For this class of service, a "Second SLA Credit" is an amount equal to 25% of the monthly Service Offering recurring or metered (as applicable) subscription charges invoiced by VMware in the calendar month for which the SLA Credit is due. Any Second SLA Credit is in lieu of any First SLA Credit that might have been otherwise due.

  For Object Storage powered by Google Cloud Platform (Durable Reduced Availability) and Object Storage powered by Google Cloud Platform (Nearline Storage):

  - If the Availability of one of these classes of service that you purchase is less than the associated Availability Commitment, but does not exceed Unavailability of more than 2232 minutes total, in a given calendar month, then you may request one (1) First SLA Credit. For these classes of service, a "First SLA Credit" is an amount equal to 25% of the monthly Service Offering recurring or metered (as applicable) subscription charges invoiced by VMware for the affected class of service in the calendar month for which the SLA Credit is due.
  - If one of these classes of service that you purchase is Unavailable for more than 2232 minutes total in a given calendar month, then you may request a Second SLA Credit. For these classes of service, a "Second SLA Credit" is an amount equal to 50% of the monthly Service Offering recurring or metered (as applicable) subscription charges invoiced by VMware for the affected class of service in the calendar month for which the SLA Credit is due. Any Second SLA Credit is in lieu of any First SLA Credit that might have been otherwise due.

Service Level Agreement Limitations

The following will be excluded from any time-based calculations related to a class of service being Unavailable: (i) scheduled maintenance windows where you have been notified at least 24 hours in advance, (ii) recurring or zero impact maintenance windows that are made generally available to all customers, (iii) your misuse of a particular class of service, (iv) force majeure events, denial of service attacks, virus or hacking attacks for which there is no commercially reasonable, known solution, or any other events that are not within our direct control or that could not have been avoided with commercially reasonable care, (v) packet loss, network or internet problems beyond VMware's border router supporting our public internet connectivity, or (vi) bugs in code, hardware, or services for which there is no commercially reasonable, known fix (even if there is a known workaround).

You will not be eligible to receive a Service Credit if: (i) your service account has any payments for the Service Offering delinquent, (ii) you are in violation of Section 3 of the Terms of Service during the time of the SLA Event, or (iii) the SLA Event was due to your failure to meet your security responsibilities as set forth in the Terms of Service.

VMware's monitoring tools, data and records will be the sole source of information used to track and validate Availability. Upon request, VMware will provide to you, within 45 days after a confirmed SLA Event (but no more than once per calendar year), a copy of the Availability report that VMware makes generally available to customers.

Search

Service Level Agreement Claims

In order to request any Service Credit, you must file a support request at https://my.vmware.com (https://my.vmware.com) within sixty (60) days of the suspected SLA Event. VMware will review the request and issue a Service Credit when VMware validates the SLA Event based on VMware's data and records.

Service Credits will be issued to the person or entity that VMware invoices for the applicable instance of the Service Offering, as a separate credit memo that can be applied towards a future invoice for that Service Offering instance. If your subscription term for the Service Offering expires or is terminated prior to the issuance of a Service Credit, the Service Credit will become void as of the date of the expiration or termination.

The Service Credits specified in this SLA are your sole and exclusive remedies for any SLA Events occurring during your subscription term for the Service Offering or for any other claim in connection with this SLA.

CONTACT SALES (/COMPANY/CONTACT_SALES.HTML) GET SUPPORT (/SUPPORT.HTML)
ABOUT VMWARE (/COMPANY.HTML) CAREERS (HTTPS://CAREERS.VMWARE.COM)

© 2017 VMware, Inc

Terms of Use (/help/legal.html)
Privacy (/help/privacy.html)
Accessibility (/help/accessibility.html)
Site Index (/site_index.html)
Trademarks (/help/trademarks.html)
Help (/help.html)
Feedback

(https://twitter.com/VMware) (https://www.facebook.com/vmware) (https://www.linkedin.com/company/vmware) (http://www.youtube.com/user/vmwaretv) (https://plus.google.com/+vmware)

(/)

(/)

vmware airwatch

AIRWATCH HOSTED SERVICES POLICY

1 ***Applicability***. This AirWatch Hosted Services Policy (this "**Policy**") governs the delivery of services to host, on Customer's behalf, the Software to enable Customer's use of the Software in a production environment via internet-based consoles ("**Hosted Services**"). In connection with any Software licenses for trial, evaluation, or testing of the Software, the Software and any Hosted Services are provided "AS IS" with no warranties, credits or SLAs of any kind. Capitalized terms, unless otherwise defined here, shall have the meanings set forth in the End User License Agreement ("EULA") or other applicable agreement between AirWatch and Customer.

2 ***Systems Management***. AirWatch shall: (i) provide all necessary hardware for the hosting of the Software (the "**AirWatch Servers**"); (ii) monitor and maintain the AirWatch Servers and provide continuous connectivity, availability, and operation of the host servers necessary to achieve the Service Levels set forth herein; and (iii) monitor hardware, systems software, and environmental controls and, based on detected problems or issues, take reasonable actions as necessary to achieve the Service Levels set forth herein.

3 ***Availability***. AirWatch shall maintain the availability of the AirWatch Servers hosting the Software on behalf of Customer ("**Availability**") to allow Customer the ability remotely access ("**Access**") the AirWatch Servers 99.9% of the calendar month, excluding any period of time designated by AirWatch during which AirWatch may limit or suspend Access to the AirWatch Server and/or Software so that AirWatch may perform routine or emergency maintenance (a "**Maintenance Window**"). AirWatch shall provide at least five (5) days' advance notice via email of Maintenance Windows or if, under the circumstances, five (5) days' notice is not practical, AirWatch shall provide as much advance notice via email as is reasonably possible.

4 ***Hosted Services Service Levels and Remedies***. AirWatch warrants it will provide Availability of the Hosted Services 99.9% of the calendar month (the "**Service Level**"). To the extent that the Hosted Services fail to conform to the Service Level, Customer may request service credits ("**Outage Credits**") as provided herein. A failure or lack of Availability for any period of time of at least one minute during which Customer is unable to utilize the Hosted Services due to AirWatch's failure to provide Customer with the specified services constitutes an "**Outage**". All Outage measurements will be rounded up or down to the nearest one minute increment, with increments equal to or greater than 30 seconds being rounded up to the next minute. Outage Credits are based on cumulative periods of Outage over a calendar month. Final determinations of the length of the cumulative periods of Outage over a calendar month shall be based on AirWatch's internal monitoring equipment and records. Outage Credits will be taken against only the Hosted Service fees for the month in which the Outage occurred. Outage Credits will be calculated in accordance with the following table:

Cumulative duration of Outage periods within a particular calendar month	Percentage of the Hosted Services fees to be credited as an Outage Credit
45 minutes through 3 hours, 36 minutes	10%
3 hours, 37 minutes through 7 hours, 12 minutes	20%
Greater than 7 hours, 12 minutes	30%

5 ***Claiming Outage Credits***. Customer must request any Outage Credit potentially due hereunder within ninety (90) days of end of the calendar month in which such Outage occurs. Customer waives any right to Outage Credits not requested within such ninety (90) day period. Outage Credits will be issued once the duration of the Outage has been validated by AirWatch. Other than termination rights, if any, the Outage Credits provide Customer's sole and exclusive remedy for any interruptions, deficiencies, or failures of any kind of the Hosted Services. The Outage Credits will not apply in the case of an Excluded Event. "**Excluded Event**" means any event that adversely impacts the Hosted Services to the extent it is caused by (a) the acts or omissions of Customer, its employees, customers, contractors, or agents; (b) the failure or malfunction of equipment, applications or systems not owned or controlled by AirWatch; (c) force majeure events; (d) a Maintenance Window; (e) any permitted suspension of Hosted Services for late payment or nonpayment; or (f) the unavailability of any Customer personnel required to restore Hosted Services, including as a result of Customer's failure to provide AirWatch with accurate, current contact information. Notwithstanding the foregoing, in the event Customer purchases Hosted Services via a Reseller, customer will seek such Outage Credits from the Reseller.

vmware airwatch

6 ***General Restrictions.*** Customer will not, and will not permit any third party, to, as solely determined by AirWatch: (a) use the Hosted Services to violate or encourage the violation of the rights of others (including intellectual property rights); (b) use the Hosted Services to engage in, advertise or deliver gambling, pornographic, or illegal activities; (c) circumvent or violate the restrictions of the Hosted Services as described in this Agreement; (d) reverse engineer, or otherwise attempt to derive source code from the Hosted Services, unless AirWatch makes the source code publicly available; (e) disable, interfere with, disrupt, or circumvent any aspect of the Hosted Services, including the integrity or performance of the Hosted Services, or third-party content or data provided through the Hosted Services; (f) access or use the Hosted Services in a way intended to avoid recurring fees or exceeding usage limits; or (g) resell or sublicense the Hosted Services. Customer must ensure that Users comply with the terms of this Policy, and Customer agrees that if Customer becomes aware of any violation by a User, Customer will terminate that User's access to Customer Content immediately. If AirWatch has reason to believe that Customer or Users have breached this Policy, AirWatch or AirWatch's designated agent may review Customer's use of the Hosted Services, including Customer's account, Customer Content and records, to verify Customer compliance with the EULA and this Policy.

7 ***Lawful Content.*** Customer will take steps to ensure that Users do not post content that: (a) may create a risk of harm, loss, physical or mental injury, emotional distress, death, disability, disfigurement, or physical or mental illness to anyone; (b) may create a risk of any other loss or damage to any person or property; (c) may constitute or contribute to a crime or tort; (d) contains any information or content that is illegal, unlawful, harmful, abusive, pornographic, racially or ethnically offensive, defamatory, infringing, invasive of personal privacy or publicity rights, harassing, humiliating to other people (publicly or otherwise), libelous, or threatening; or (e) contains any information or content that Customer does not have a right to make available under any law or under contractual or fiduciary relationships. Customer represents and warrants that the Customer Content does not and will not violate any third-party rights, including any intellectual property rights, and rights of publicity and privacy.

8 ***Sensitive Data Restrictions.*** Neither Customer nor Users will use the Hosted Service to transmit, store or process: (i) any patient, medical or other protected health information, whether regulated by HIPAA or any similar federal or state laws, rules or regulations; (ii) financial account information or payment card data; or (iii) any other information subject to regulation or protection under specific laws such as the Gramm-Leach-Bliley Act (or related rules or regulations) ((i) through (iii), collectively, "Sensitive Data"). "HIPAA" means the Health Insurance Portability and Accountability Act, as amended and supplemented. AirWatch does not intend use of the Hosted Service to create obligations under HIPAA, and AirWatch makes no representations that the Hosted Service satisfies HIPAA requirements. If Customer is (or Customer becomes) a Covered Entity or Business Associate, as defined in HIPAA, Customer agrees not to use the Hosted Service for any purpose or in any manner involving Protected Health Information (as defined in HIPAA) unless Customer has received prior written consent for such use from AirWatch. Customer acknowledges and agrees that use of the Hosted Services to transmit, process or store Sensitive Data is not necessary for use of the Software. Customer shall be solely responsible for any such use of Sensitive Data with the Hosted Service by Customer or Users and Customer will hold harmless AirWatch for the same. Customer will not include in Customer Content any Classified Information, as that term is defined in the National Industrial Security Program Operating Manual.

9 ***Violations of Acceptable Use.*** If Customer becomes aware that any of the Customer Content or User's use of the Customer Content violates these acceptable use restrictions, Customer will immediately suspend and remove the applicable part of the Customer Content or suspend the User's access to the Hosted Service. If Customer fails to do so, AirWatch may ask Customer to do so. If Customer fails to comply with AirWatch's request within twenty-four hours, AirWatch may suspend Customer's account or disable access to the Hosted Service until Customer complies with AirWatch's request.

10 ***Customer Content.*** AirWatch may access and use Customer Content only as necessary to provide the Hosted Service (which AirWatch may do with the assistance of Affiliates, service providers and contractors), perform or enforce contractual obligations, or comply with applicable law. For instance, AirWatch may need to access or use Customer Content (or provide to one of our Affiliates, service providers or contractors) to: (a) prevent or address service or technical problems; (b) provide customer support; (c) detect, prevent or address fraud, technology or security issues; or (d); respond to a subpoena, warrant, audit or agency action or other law enforcement request.

vmware airwatch

11 ***Data Processing Instructions.*** Personal Data that AirWatch receives is dependent upon Customer's configuration settings. To provide the Hosted Services to Customer, AirWatch may process Customer Personal Data for the purposes described above or otherwise in accordance with Customer's lawful instructions, which, together with the EULA, are Customer's complete and final instructions to AirWatch in relation to processing of Customer Personal Data. Customer acknowledges that it is the controller of Customer Personal Data and that AirWatch will process the Customer Personal Data only as a processor on Customer's behalf. AirWatch will not divulge any Customer Personal Data to any person, except to the extent necessary for the proper performance or otherwise in accordance with this Agreement or Customer's lawful instructions.

12 ***Security of Content Data.*** AirWatch will implement appropriate technical and organizational measures to protect AirWatch's infrastructure and networks. Without prejudice to Customer's security responsibilities in this Policy, these measures will help to protect Customer Content against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing. Customer will properly configure and use the Hosted Service so that it is suitable for Customer's use and in accordance with Customer's obligations under this Policy. Customer will maintain appropriate security, protection and backups of Customer Content and will camouflage or securely encrypt Customer Content in a manner compatible with the Hosted Services whenever possible. Customer is responsible for any losses or other consequences arising from Customer's failure to encrypt or back up Customer Content.

13 ***SSAE16.*** During the Term, AirWatch will maintain its Statement on Standards for Attestation Engagements No.16 Type II report or a comparable report applicable to the Hosted Service, which will be updated on a regular basis by qualified and independent party auditors. Upon Customer's written request during the term and subject to AirWatch's security policies, AirWatch will provide Customer with the summary report or other information as may be reasonably requested by Customer regarding its data security obligations under this Policy and under any applicable agreements between Customer and AirWatch.

14 ***Privacy and Children.*** AirWatch is not intended for children under the age of thirteen (13) in the USA or under the age of sixteen (16) in the European Economic Area (unless a Member State permits a lower age of thirteen (13)). Unless Customer has received prior written consent for such use, Customer shall not direct children under the applicable statutory age of consent to use the Hosted Service or otherwise use the Hosted Service to collect, disclosure, publish or store information about children under the legal age of consent where prohibited by applicable law.

15 ***Education Customers.*** Hosted Services provided to education sector customers are subject to AirWatch's then-current Educational Software Rider, the current version of which is available at http://www.air-watch.com/downloads/legal/201507EducationalSoftwareRider.pdf.

Attachment A, Exhibit 1

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls that party, and here "control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of that entity.

1.2 "Documentation" means that documentation that is generally provided to You by VMware with the Software, as revised by VMware from time to time, and which may include end user manuals, operation instructions, installation guides, release notes, and on-line help files regarding the use of the Software.

1.3 "Guest Operating Systems" means instances of third-party operating systems licensed by You, installed in a Virtual Machine and run using the Software.

1.4 "Intellectual Property Rights" means all worldwide intellectual property rights, including without limitation, copyrights, trademarks, service marks, trade secrets, know how, inventions, patents, patent applications, moral rights and all other proprietary rights, whether registered or unregistered.

1.5 "License" means a license granted under Section 2.1 (General License Grant).

1.6 "License Key" means a serial number that enables You to activate and use the Software.

1.7 "License Term" means the duration of a License as specified in the Order.

1.8 "License Type" means the type of License applicable to the Software, as more fully described in the Order.

1.9 "Open Source Software" or "OSS" means software components embedded in the Software and provided under separate license terms, which can be found either in the open_source_licenses.txt file (or similar file) provided within the Software or at www.vmware.com/download/open_source.html.

1.10 "Order" means a purchase order, enterprise license agreement, or other ordering document issued by You to VMware or a VMware authorized reseller that references and incorporates this EULA and is accepted by VMware as set forth in Section 4 (Order).

1.11 "Product Guide" means the current version of the VMware Product Guide at the time of Your Order, copies of which are found at www.vmware.com/download/eula.

1.12 "Support Services Terms" means VMware's then-current support policies, copies of which are posted at www.vmware.com/support/policies.

1.13 "Software" means the VMware Tools and the VMware computer programs listed on VMware's commercial price list to which You acquire a license under an Order, together with any software code relating to the foregoing that is provided to You pursuant to a support and subscription service contract and that is not subject to a separate license agreement.

1.14 "Territory" means the country or countries in which You have been invoiced; provided, however, that if You have been invoiced within any of the European Economic Area member states, You may deploy the corresponding Software throughout the European Economic Area.

1.15 "Third Party Agent" means a third party delivering information technology services to You pursuant to a written contract with You.

1.16 "Virtual Machine" means a software container that can run its own operating system and execute applications like a physical machine.

1.17 "VMware" means VMware, Inc., a Delaware corporation, if You are purchasing Licenses or services for use in the United States and VMware International Limited, a company organized and existing under the laws of Ireland, for all other purchases.

1.18 "VMware Tools" means the suite of utilities and drivers, Licensed by VMware under the "VMware Tools" name, that can be installed in a Guest Operating System to enhance the performance and functionality of a Guest Operating System when running in a Virtual Machine.

2. LICENSE GRANT.

2.1 General License Grant. VMware grants to You a non-exclusive, non-transferable (except as set forth in Section 12.1 (Transfers; Assignment) license to use the Software and the Documentation during the period of the license and within the Territory, solely for Your internal business operations, and subject to the provisions of the Product Guide. Unless otherwise indicated in the Order, licenses granted to You will be perpetual, will be for use of object code only, and will commence on either delivery of the physical media or the date You are notified of availability for electronic download.

2.2 Third Party Agents. Under the License granted to You in Section 2.1 (General License Grant) above, You may permit Your Third Party Agents to access, use and/or operate the Software on Your behalf for the sole purpose of delivering services to You, provided that You will be fully responsible for Your Third Party Agents' compliance with terms and conditions of this EULA and any breach of this EULA by a Third Party Agent shall be deemed to be a breach by You.

2.3 Copying Permitted. You may copy the Software and Documentation as necessary to install and run the quantity of copies licensed, but otherwise for archival purposes only.

2.4 Benchmarking. You may use the Software to conduct internal performance testing and benchmarking studies. You may only publish or otherwise distribute the results of such studies to third parties as follows: (a) if with respect to VMware's Workstation or Fusion products, only if You provide a copy of Your study to benchmark@vmware.com prior to distribution; (b) if with respect to any other Software, only if VMware has reviewed and approved of the methodology, assumptions and other parameters of the study (please contact VMware at benchmark@vmware.com to request such review and approval) prior to such publication and distribution.

2.5 VMware Tools. You may distribute the VMware Tools to third parties solely when installed in a Guest Operating System within a Virtual Machine. You are liable for compliance by those third parties with the terms and conditions of this EULA.

2.6 Open Source Software. Notwithstanding anything herein to the contrary, Open Source Software is licensed to You under such OSS's own applicable license terms, which can be found in the open_source_licenses.txt file, the Documentation or as applicable, the corresponding source files for the Software available at www.vmware.com/download/open_source.html. These OSS license terms are consistent with the license granted in Section 2 (License Grant), and may contain additional rights benefiting You. The OSS license terms shall take precedence over this EULA to the extent that this EULA imposes greater restrictions on You than the applicable OSS license terms. To the extent the license for any Open Source Software requires VMware to make available to You the corresponding source code and/or modifications (the "Source Files"), You may obtain a copy of the applicable Source Files from VMware's website at www.vmware.com/download/open_source.html or by sending a written request, with Your name and address to: VMware, Inc., 3401 Hillview Avenue, Palo Alto, CA 94304, United States of America. All requests should clearly specify: Open Source Files Request, Attention: General Counsel. This offer to obtain a copy of the Source Files is valid for three years from the date You acquired this Software.

3. RESTRICTIONS; OWNERSHIP.

3.1 License Restrictions. Without VMware's prior written consent, You must not, and must not allow any third party to: (a) use Software in an application services provider, service bureau, or similar capacity for third parties, except that You may use the Software to deliver hosted services to Your Affiliates; (b) disclose to any third party the results of any benchmarking testing or comparative or competitive analyses of VMware's Software done by or on behalf of You, except as specified in Section 2.4 (Benchmarking); (c) make available Software in any form to anyone other than Your employees or contractors reasonably acceptable to VMware and require access to use Software on behalf of You in a matter permitted by this EULA, except as specified in Section 2.2 (Third Party Agents); (d) transfer or sublicense Software or Documentation to an Affiliate or any third party, except as expressly permitted in Section 12.1 (Transfers; Assignment); (e) use Software in conflict with the terms and restrictions of the Software's licensing model and other requirements specified in Product Guide and/or VMware quote; (f) except to the extent permitted by applicable mandatory law, modify, translate, enhance, or create derivative works from the Software, or reverse engineer, decompile, or otherwise attempt to derive source code from the Software, except as specified in Section 3.2 (Decompilation); (g) remove any copyright or other proprietary notices on or in any copies of Software; or (h) violate or circumvent any technological restrictions within the Software or specified in this EULA, such as via software or services.

3.2 Decompilation. Notwithstanding the foregoing, decompiling the Software is permitted to the extent the laws of the Territory give You the express right to do so to obtain information necessary to render the Software interoperable with other software; provided, however, You must first request such information from VMware, provide all reasonably requested information to allow VMware to assess Your claim, and VMware may, in its discretion, either provide such interoperability information to You, impose reasonable conditions, including a reasonable fee, on such use of the Software, or offer to provide alternatives to ensure that VMware's proprietary rights in the Software are protected and to reduce any adverse impact on VMware's proprietary rights.

3.3 Ownership. The Software and Documentation, all copies and portions thereof, and all improvements, enhancements, modifications and derivative works thereof, and all Intellectual Property Rights therein, are and shall remain the sole and exclusive property of VMware and its licensors. Your rights to use the Software and Documentation shall be limited to those expressly granted in this EULA and any applicable Order. No other rights with respect to the Software or any related Intellectual Property Rights are implied. You are not authorized to use (and shall not permit any third party to use) the Software, Documentation or any portion thereof except as expressly authorized by this EULA or the applicable Order. VMware reserves all rights not expressly granted to You. VMware does not transfer any ownership rights in any Software.

3.4 Guest Operating Systems. Certain Software allows Guest Operating Systems and application programs to run on a computer system. You acknowledge that You are responsible for obtaining and complying with any licenses necessary to operate any such third-party software.

4. ORDER. Your Order is subject to this EULA. No Orders are binding on VMware until accepted by VMware. Orders for Software are deemed to be accepted upon VMware's delivery of the Software included in such Order. Orders issued to VMware do not have to be signed to be valid and enforceable.

5. RECORDS AND AUDIT. During the License Term for Software and for two (2) years after its expiration or termination, You will maintain accurate records of Your use of the Software sufficient to show compliance with the terms of this EULA. During this period, VMware will have the right to audit Your use of the Software to confirm compliance with the terms of this EULA. That audit is subject to reasonable notice by VMware and will not unreasonably interfere with Your business activities. VMware may conduct no more than one (1) audit in any twelve (12) month period, and only during normal business hours. You will reasonably cooperate with VMware and any third party auditor and will, without prejudice to other rights of VMware, address any non-compliance identified by the audit by promptly paying additional fees. You will promptly reimburse VMware for all reasonable costs of the audit if the audit reveals either underpayment of more than five (5%) percent of the Software fees payable by You for the period audited, or that You have materially failed to maintain accurate records of Software use.

6. SUPPORT AND SUBSCRIPTION SERVICES. Except as expressly specified in the Product Guide, VMware does not provide any support or subscription services for the Software under this EULA. You have no rights to any updates, upgrades or extensions or enhancements to the Software developed by VMware unless you separately purchase VMware support or subscription services. These support or subscription services are subject to the Support Services Terms.

7. WARRANTIES.

7.1 Software Warranty, Duration and Remedy. VMware warrants to You that the Software will, for a period of ninety (90) days following notice of availability for electronic download or delivery ("Warranty Period"), substantially conform to the applicable Documentation, provided that the Software: (a) has been properly installed and used at all times in accordance with the applicable Documentation; and (b) has not been modified or added to by persons other than VMware or its authorized representative. VMware will, at its own expense and as its sole obligation and Your exclusive remedy for any breach of this warranty, either replace that Software or correct any reproducible error in that Software reported to VMware by You in writing during the Warranty Period. If VMware determines that it is unable to correct the error or replace the Software, VMware will refund to You the amount paid by You for that Software, in which case the License for that Software will terminate.

7.2 Software Disclaimer of Warranty. OTHER THAN THE WARRANTY ABOVE, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VMWARE AND ITS SUPPLIERS MAKE NO OTHER EXPRESS WARRANTIES UNDER THIS EULA, AND DISCLAIM ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ANY WARRANTY ARISING BY STATUTE, OPERATION OF LAW, COURSE OF DEALING OR PERFORMANCE, OR USAGE OF TRADE. VMWARE AND ITS LICENSORS DO NOT WARRANT THAT THE SOFTWARE WILL OPERATE UNINTERRUPTED OR THAT IT WILL BE FREE FROM DEFECTS OR THAT IT WILL MEET YOUR REQUIREMENTS.

8. INTELLECTUAL PROPERTY INDEMNIFICATION.

8.1 Defense and Indemnification. Subject to the remainder of this Section 8 (Intellectual Property Indemnification), VMware shall defend You against any third party claim that the Software infringes any patent, trademark or copyright of such third party, or misappropriates a trade secret (but only to the extent that the misappropriation is not a result of Your actions) under the laws of: (a) the United States and Canada; (b) the European Economic Area; (c) Australia; (d) New Zealand; (e) Japan; or (f) the People's Republic of China, to

the extent that such countries are part of the Territory for the License ("Infringement Claim") and indemnify You from the resulting costs and damages finally awarded against You to such third party by a court of competent jurisdiction or agreed to in settlement. The foregoing obligations are applicable only if You: (i) promptly notify VMware in writing of the Infringement Claim; (ii) allow VMware sole control over the defense for the claim and any settlement negotiations; and (iii) reasonably cooperate in response to VMware requests for assistance. You may not settle or compromise any Infringement Claim without the prior written consent of VMware.

8.2 Remedies. If the alleged infringing Software become, or in VMware's opinion be likely to become, the subject of an Infringement Claim, VMware will, at VMware's option and expense, do one of the following: (a) procure the rights necessary for You to make continued use of the affected Software; (b) replace or modify the affected Software to make it non-infringing; or (c) terminate the License to the affected Software and discontinue the related support services, and, upon Your certified deletion of the affected Software, refund: (i) the fees paid by You for the License to the affected Software, less straight-line depreciation over a three (3) year useful life beginning on the date such Software was delivered; and (ii) any pre-paid service fee attributable to related support services to be delivered after the date such service is stopped. Nothing in this Section 8.2 (Remedies) shall limit VMware's obligation under Section 8.1 (Defense and Indemnification) to defend and indemnify You, provided that You replace the allegedly infringing Software upon VMware's making alternate Software available to You and/or You discontinue using the allegedly infringing Software upon receiving VMware's notice terminating the affected License.

8.3 Exclusions. Notwithstanding the foregoing, VMware will have no obligation under this Section 8 (Intellectual Property Indemnification) or otherwise with respect to any claim based on: (a) a combination of Software with non-VMware products (other than non-VMware products that are listed on the Order and used in an unmodified form); (b) use for a purpose or in a manner for which the Software was not designed; (c) use of any older version of the Software when use of a newer VMware version would have avoided the infringement; (d) any modification to the Software made without VMware's express written approval; (e) any claim that relates to open source software or freeware technology or any derivatives or other adaptations thereof that is not embedded by VMware into Software listed on VMware's commercial price list; or (f) any Software provided on a no charge, beta or evaluation basis. THIS SECTION 8 (INTELLECTUAL PROPERTY INDEMNIFICATION) STATES YOUR SOLE AND EXCLUSIVE REMEDY AND VMWARE'S ENTIRE LIABILITY FOR ANY INFRINGEMENT CLAIMS OR ACTIONS.

9. LIMITATION OF LIABILITY.

9.1 Limitation of Liability. TO THE MAXIMUM EXTENT MANDATED BY LAW, IN NO EVENT WILL VMWARE AND ITS LICENSORS BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE, LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY, OR OTHERWISE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE PRECEDING LIMITATION MAY NOT APPLY TO YOU. VMWARE'S AND ITS LICENSORS' LIABILITY UNDER THIS EULA WILL NOT, IN ANY EVENT, REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE, EXCEED THE GREATER OF THE LICENSE FEES YOU PAID FOR THE SOFTWARE GIVING RISE TO THE CLAIM OR $5000. THE FOREGOING LIMITATIONS SHALL APPLY REGARDLESS OF WHETHER VMWARE OR ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

9.2 Further Limitations. VMware's licensors shall have no liability of any kind under this EULA and VMware's liability with respect to any third party software embedded in the Software shall be subject to Section 9.1 (Limitation of Liability). You may not bring a claim under this EULA more than eighteen (18) months after the cause of action arises.

10. TERMINATION.

10.1 EULA Term. The term of this EULA begins on the notice of availability for electronic download or delivery of the Software and continues until this EULA is terminated in accordance with this Section 10.

10.2 Termination for Breach. VMware may terminate this EULA effective immediately upon written notice to You if: (a) You fail to pay any portion of the fees under an applicable Order within ten (10) days after receiving written notice from VMware that payment is past due; or (b) You breach any other provision of this EULA and fail to cure within thirty (30) days after receipt of VMware's written notice thereof.

10.3 Termination for Insolvency. VMware may terminate this EULA effective immediately upon written notice to You if You: (a) terminate or suspend your business; (b) become insolvent, admit in writing Your inability to pay Your debts as they mature, make an assignment for the benefit of creditors; or become subject to control of a trustee, receiver or similar authority; or (c) become subject to any bankruptcy or insolvency proceeding.

10.4 Effect of Termination. Upon VMware's termination of this EULA: (a) all Licensed rights to all Software granted to You under this EULA will immediately cease; and (b) You must cease all use of all Software, and return or certify destruction of all Software and License Keys (including copies) to VMware, and return, or if requested by VMware, destroy, any related VMware Confidential Information in Your possession or control and certify in writing to VMware that You have fully complied with these requirements. Any provision will survive any termination or expiration if by its nature and context it is intended to survive, including Sections 1 (Definitions), 2.6 (Open Source Software), 3 (Restrictions; Ownership), 5 (Records and Audit), 7.2 (Software Disclaimer of Warranty), 9 (Limitation of Liability), 10 (Termination), 11 (Confidential Information) and 12 (General).

11. CONFIDENTIAL INFORMATION.

11.1 Definition. "Confidential Information" means information or materials provided by one party (" **Discloser**") to the other party ("Recipient") which are in tangible form and labelled "confidential" or the like, or, information which a reasonable person knew or should have known to be confidential. The following information shall be considered Confidential Information whether or not marked or identified as such: (a) License Keys; (b) information regarding VMware's pricing, product roadmaps or strategic marketing plans; and (c) non-public materials relating to the Software.

11.2 Protection. Recipient may use Confidential Information of Discloser; (a) to exercise its rights and perform its obligations under this EULA; or (b) in connection with the parties' ongoing business relationship. Recipient will not use any Confidential Information of Discloser for any purpose not expressly permitted by this EULA, and will disclose the Confidential Information of Discloser only to the employees or contractors of Recipient who have a need to know such Confidential Information for purposes of this EULA and who are under a duty of confidentiality no less restrictive than Recipient's duty hereunder. Recipient will protect Confidential Information from unauthorized use, access, or disclosure in the same manner as Recipient protects its own confidential or proprietary information of a similar nature but with no less than reasonable care.

11.3 Exceptions. Recipient's obligations under Section 11.2 (Protection) with respect to any Confidential Information will terminate if Recipient can show by written records that such information: (a) was already known to Recipient at the time of disclosure by Discloser; (b) was disclosed to Recipient by a third party who had the right to make such disclosure without any confidentiality restrictions; (c) is, or through no fault of Recipient has become, generally available to the public; or (d) was independently developed by Recipient without access to, or use of, Discloser's Information. In addition, Recipient will be allowed to disclose Confidential Information to the extent that such disclosure is required by law or by the order of a court of similar judicial or administrative body, provided that Recipient notifies Discloser of such required disclosure promptly and in writing and cooperates with Discloser, at Discloser's request and expense, in any lawful action to contest

or limit the scope of such required disclosure.

11.4 Data Privacy. You agree that VMware may process technical and related information about Your use of the Software which may include internet protocol address, hardware identification, operating system, application software, peripheral hardware, and non-personally identifiable Software usage statistics to facilitate the provisioning of updates, support, invoicing or online services and may transfer such information to other companies in the VMware worldwide group of companies from time to time. To the extent that this information constitutes personal data, VMware shall be the controller of such personal data. To the extent that it acts as a controller, each party shall comply at all times with its obligations under applicable data protection legislation.

12. GENERAL.

12.1 Transfers; Assignment. Except to the extent transfer may not legally be restricted or as permitted by VMware's transfer and assignment policies, in all cases following the process set forth at www.vmware.com/support/policies/licensingpolicies.html, You will not assign this EULA, any Order, or any right or obligation herein or delegate any performance without VMware's prior written consent, which consent will not be unreasonably withheld. Any other attempted assignment or transfer by You will be void. VMware may use its Affiliates or other sufficiently qualified subcontractors to provide services to You, provided that VMware remains responsible to You for the performance of the services.

12.2 Notices. Any notice delivered by VMware to You under this EULA will be delivered via mail, email or fax.

12.3 Waiver. Failure to enforce a provision of this EULA will not constitute a waiver.

12.4 Severability. If any part of this EULA is held unenforceable, the validity of all remaining parts will not be affected.

12.5 Compliance with Laws; Export Control; Government Regulations. Each party shall comply with all laws applicable to the actions contemplated by this EULA. You acknowledge that the Software is of United States origin, is provided subject to the U.S. Export Administration Regulations, may be subject to the export control laws of the applicable territory, and that diversion contrary to applicable export control laws is prohibited. You represent that (1) you are not, and are not acting on behalf of, (a) any person who is a citizen, national, or resident of, or who is controlled by the government of any country to which the United States has prohibited export transactions; or (b) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List; and (2) you will not permit the Software to be used for, any purposes prohibited by law, including, any prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons. The Software and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation", respectively, pursuant to DFARS Section 227.7202 and FAR Section 12.212(b), as applicable. Any use, modification, reproduction, release, performing, displaying or disclosing of the Software and documentation by or for the U.S. Government shall be governed solely by the terms and conditions of this EULA.

12.6 Construction. The headings of sections of this EULA are for convenience and are not to be used in interpreting this EULA. As used in this EULA, the word 'including' means "including but not limited to".

12.7 Governing Law. This EULA is governed by the laws of the State of California, United States of America (excluding its conflict of law rules), and the federal laws of the United States. To the extent permitted by law, the state and federal courts located in Santa Clara County, California will be the exclusive jurisdiction for disputes arising out of or in connection with this EULA. The U.N. Convention on Contracts for the International Sale of Goods does not apply.

12.8 Third Party Rights. Other than as expressly set out in this EULA, this EULA does not create any rights for any person who is not a party to it, and no person who is not a party to this EULA may enforce any of its

terms or rely on any exclusion or limitation contained in it.

12.9 Order of Precedence. In the event of conflict or inconsistency among the Product Guide, this EULA and the Order, the following order of precedence shall apply: (a) the Product Guide, (b) this EULA and (c) the Order. With respect to any inconsistency between this EULA and an Order, the terms of this EULA shall supersede and control over any conflicting or additional terms and conditions of any Order, acknowledgement or confirmation or other document issued by You.

12.10 Entire Agreement. This EULA, including accepted Orders and any amendments hereto, and the Product Guide contain the entire agreement of the parties with respect to the subject matter of this EULA and supersede all previous or contemporaneous communications, representations, proposals, commitments, understandings and agreements, whether written or oral, between the parties regarding the subject matter hereof. This EULA may be amended only in writing signed by authorized representatives of both parties.

12.11 Contact Information. Please direct legal notices or other correspondence to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America, Attention: Legal Department.

vRealize Air

(/)

Terms of Service

Last updated: July 14, 2015

By accessing the VMware hosted service specified in your Order (the " **Service Offering**"), you agree to be bound by these terms of service between you and VMware (" **Agreement**"). This Agreement also includes the applicable Service Description, Privacy Addendum, Support Policy, and Service Level Agreement. If you do not agree to this Agreement, you must not access the Service Offering. " **You**" means you individually or the entity that you represent. If you are entering into this Agreement for an entity, you represent to us that you have legal authority to bind that entity. " **VMware**," " **we**," or " **us**" means VMware, Inc., a Delaware corporation, to the extent that you purchase the Service Offering in the United States, VMware vCloud Service G.K., a company organized and existing under the laws of Japan, to the extent that you purchase the Service Offering in Japan, and VMware International Limited, a company organized and existing under the laws of Ireland, to the extent that you purchase the Service Offering elsewhere. Capitalized terms used in this Agreement are defined throughout this Agreement and in Section 14.

1. The Service Offering.

1.1 Generally. This Agreement governs your access to and use of the Service Offering. We may deliver the Service Offering to you with the assistance of our affiliates, licensors and service providers. You will comply with all laws, rules and regulations applicable to your use of the Service Offering. You also will comply with the applicable Service Description, Privacy Addendum, and Support Policy. If you access the Service Offering, or any of its features or functionality, on an evaluation or beta basis, please see Section 1.5 for other terms that apply to you.

1.2 Access to the Service Offering. You may access and use the Service Offering solely for your own benefit and only in accordance with this Agreement. To access the Service Offering, you must register for the Service Offering and set up an authorized account with Login Credentials. You may monitor and manage your Service Offering account via the My VMware Portal available at https://my.vmware.com/group/vmware/home (https://my.vmware.com/group/vmware/home) and through the Service Offering Portal available in the Order. You must keep confidential your Login Credentials. If you set up an authorized account for an organization, you must require that all authorized Users of that account (including anyone providing services to you) keep confidential their Login Credentials. You must keep your registration information accurate, complete and current for as long as you use the Service Offering. You are responsible for any use that occurs under your Login Credentials, including any activities by you or your employees, contractors or agents. If you believe an unauthorized person has gained access to your Login Credentials, you must notify us as soon as possible by submitting a Severity 1 Service Request (see the applicable Support Policy).

1.3 Verifying Compliance; Cooperation. We have the right to verify your compliance with this Agreement. If we seek to verify that compliance, you will provide information or other materials reasonably requested by us to assist in the verification. We monitor the overall performance and stability of the infrastructure of the Service Offering. You may not block or interfere with that monitoring. If we reasonably believe a problem with the Service Offering may be attributable to Your Content or your use of the Service Offering, you will cooperate with us to identify the source of and resolve that problem.

1.4 Third Party Content. As part of your use of the Service Offering, you may receive access to Third Party Content, which is subject to separate terms. If so, those separate terms will prevail over this Agreement as to your use of the Third Party Content. Third Party Content is available "AS IS" without indemnification, support, or warranty or condition of any kind. You are responsible for reviewing, accepting, and complying with any third party terms of use or other restrictions applicable to the Third Party Content. Those terms will be available to you through a notification within the Service Offering. We reserve the right to suspend or terminate the Third Party Content at any time. We will use commercially reasonable efforts to provide reasonable notice of that suspension or termination.

1.5 Evaluation and Beta Use. If you access the Service Offering, or a feature or functionality of the Service Offering, on an evaluation or beta basis (either referred to as the "Evaluation Service"), then you may use the Evaluation Service only for evaluation purposes and for the period we specify. You must not use the Evaluation Service for any production computing activity. Notwithstanding any other provision of this Agreement, we provide the Evaluation Service (a) free of charge and without support; and (b) "AS IS", excluding any Service Level Agreement, and without indemnification or warranty or condition of any kind. Also, certain features or services described in the Service Description may not be available for the Evaluation Service. You will not have access to Your Content or the Evaluation Service when it terminates, and the features and functionality of the Evaluation Service do not constitute an implied commitment to offer them to you or anyone as part of the Service Offering on a generally available basis.

1.6 Open Source Software. You may receive open source software when you use the Service Offering. Any open source software distributed to you is made available under the applicable open source license, which can be found at: http://www.vmware.com/download/open_source.html (/download/open_source.html). You may obtain a copy of these licenses and any source code (and modifications) that we are required to make available under these licenses (the " **Source Files**") at http://www.vmware.com/download/open_source.html (/download/open_source.html) or by sending a written request, with your name and address, to: VMware, Inc., 3401 Hillview Avenue, Palo Alto, CA 94304, United States of America. All written requests must clearly specify: Open Source Files Request, Attention: General Counsel. This offer to obtain a copy of the Source Files is valid for three years from the date you last received open source software as part of the Service Offering.

2. Data Protection and Security.

2.1 Data Protection. We will process personal data contained in Your Content, and maintain appropriate technical and organizational measures (administrative, physical and technical safeguards), as set forth in the Privacy Addendum.

2.2 Your Content; Security. You are solely responsible for Your Content. Except as provided by the Privacy Addendum, You are responsible for protecting the security of Your Content, including any access to Your Content that you might provide to your employees, customers or other third parties, and when it is in transit to and from the Service Offering. The Service Offering provides you with certain software and functionality to help you protect Your Content from unauthorized access. You must take and maintain appropriate steps regarding the security, protection and backup of Your Content, which might include the use of encryption technology to protect Your Content from unauthorized access. You are responsible for providing any necessary notices to Users and for obtaining any legally-required consents from Users concerning their use of the Service Offering. You are responsible for complying with any laws or regulations that might

apply to Your Content. You are responsible for any losses or other consequences arising from your failure to encrypt or back up Your Content.

3. Acceptable Use.

3.1 General Restrictions. You and any Users accessing the Service Offering through you may not: (a) resell or sublicense the Service Offering; or (b) use or access the Service Offering: (i) in a way prohibited by law, regulation, governmental order or decree; (ii) to violate any rights of others; (iii) to try to gain unauthorized access to, test the vulnerability of, or disrupt the Service Offering or any other service, device, data, account or network; (iv) to spam or distribute malware; (v) in a way that could harm the Service Offering or impair anyone else's use of it; (vi) in a way intended to work around the Service Offering's technical limitations, recurring fees or usage limits; or (vii) in any application or situation where failure of the Service Offering could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage. You must ensure that your Users comply with the terms of this Agreement, and you agree that if you become aware of any violation by one of your Users, you will immediately terminate that User's access to Your Content. If we have reason to believe that you or your Users have breached this Agreement, we or our designated representative may review your use of the Service Offering, including your account, Your Content, and your records, to verify your compliance with this Agreement.

3.2 Content Restrictions. You will take steps to ensure that any User does not post content that: (a) may create a risk of harm, loss, physical or mental injury, emotional distress, death, disability, disfigurement, or physical or mental illness to anyone; (b) may create a risk of any other loss or damage to any person or property; (c) may constitute or contribute to a crime or tort; (d) contains any information or content that is illegal, unlawful, harmful, abusive, pornographic, racially or ethnically offensive, defamatory, infringing, invasive of personal privacy or publicity rights, harassing, humiliating to other people (publicly or otherwise), libelous, threatening, or otherwise objectionable; or (e) contains any information or content that you do not have a right to make available under any law or under contractual or fiduciary relationships. You are responsible for any software, product or service that a third party licenses, sells or makes available to you that you install or use with the Service Offering. Your use of that software, product or service is governed by separate terms between you and that third party. We are not a party to and are not bound by any of those separate terms. You represent and warrant that Your Content does not and will not violate any third-party rights, including any Intellectual Property Rights, and rights of publicity and privacy. You will ensure that your use of the Service Offering complies at all times with your privacy policies and all applicable laws and regulations, including any encryption requirements.

3.3 Violations of Acceptable Use. If you become aware that any of Your Content or any User's access to or use of Your Content violates Sections 3.1 or 3.2, you will take immediate action to remove the applicable part of Your Content or suspend the User's access. We may also ask you to take action within a certain time period, and if you fail to comply with the request, we may suspend your account pursuant to Section 6.

3.4 Notification of Infringement Concerns. If you believe that your copyrighted work has been copied and is accessible on the Service Offering in a way that constitutes copyright infringement, please send a notice to us as provided in Section 8 of the Community Terms of Use available at http://www.vmware.com/community_terms.html (/community_terms.html).

4. IP Ownership.

4.1 Ownership of Service Offering. We and our licensors own and retain all right, title and interest in and to the Service Offering and any related VMware Software, including all improvements, enhancements, modifications and derivative works thereof, and all Intellectual Property Rights therein. This includes any information that we collect and analyze in connection with the Service Offering, such as usage patterns, user feedback and other information to improve and evolve our software products and services offerings. Your rights to use the Service Offering are limited to those expressly granted in this Agreement. No other rights with respect to the Service Offering, any related VMware Software, or any related Intellectual Property Rights are implied.

4.2 Ownership of Your Content. You and your authorized Users retain all right, title and interest in and to Your Content and all Intellectual Property Rights therein. Our rights to access and use Your Content are limited to those expressly granted in this Agreement. No other rights with respect to Your Content or any related Intellectual Property Rights are implied.

4.3. Feedback. We will be free to use for any purpose any feedback (such as comments or suggestions) that you provide to us regarding the Service Offering. You hereby grant to us a non-exclusive, perpetual, irrevocable, royalty-free, transferable, worldwide right and license, with the right to sublicense, to use, reproduce, perform, display, disclose, distribute, modify, prepare derivative works of and otherwise exploit the feedback without restriction in any manner now known or in the future conceived and to make, use, sell, offer to sell, import and export any product or service that incorporates the feedback.

5. Orders, Delivery, Payment, and Taxes.

5.1 Orders Generally. All Orders issued to VMware are subject to the terms of this Agreement and are not binding until accepted by VMware. We are not required to provide any Service Offering to you until you provide all information we require for processing your Order. Your Order will be deemed accepted when we authorize the purchased Service Offering for your Login Credentials.

5.2 Delivery. When VMware accepts your Order for the Service Offering, we will deliver the corresponding Login Credentials to you by email to the address associated with your account. If VMware ships a physical object in connection with an add-on feature of the Service Offering, shipping and delivery terms are Ex Works VMware's regional fulfillment facility (INCOTERMS 2010).

5.3 Direct Orders. This Section 5.3 applies only to Orders and purchases you make directly with VMware. A VMware authorized reseller might specify similar terms when you make an Order or purchase through that reseller.

5.3.1 Purchase Orders. For Subscription-based Service Offering orders placed directly with VMware, you must issue a purchase order to VMware for the initial Service Offering order, but a purchase order is not required for us to invoice you for the monthly billings that occur after the initial Order billing.

5.3.2 Invoicing and Payment. We will bill you as specified in the Service Description. You will pay all fees for use of the Service Offering in the amount and currency specified in your invoice by one of the payment methods that we support as specified in the Service Description, and in any event no later than 30 days after the date of the invoice. For an OnDemand-based Service Offering, you will pay in arrears on a monthly basis the applicable fees based on your actual metered usage of the Service Offering. For a Subscription-based Service Offering, you will pay in advance the applicable fees for the monthly or prepaid charges due, and you will pay in arrears the initial monthly fees and for any metered usage components consumed. The applicable fees for the Service Offering will be governed by the then-current applicable price list at the time of invoicing. We may increase or add new fees for the Service Offering by notifying you at least 30 days in advance.

5.3.3 Taxes. Service Offering fees are exclusive of Taxes. "**Taxes**" means any sales, VAT, GST (Goods and Services Tax), use, gross receipts, business and occupation, and other taxes (other than taxes on our income), export and import fees, customs duties and similar charges imposed by any government or other

authority. You shall pay or reimburse us for all Taxes arising out of the transactions contemplated by this Agreement. If you are required to pay or withhold any Tax for payments due under this Agreement, you shall gross up your payment to us so that we receive sums due in full and free of any deductions. If you are required to pay any Tax to a taxing authority, you will also provide documentation to us showing that you paid those Taxes to the relevant taxing authority. You hereby confirm that we can rely on the name and address you provide to us when you agree to the Service Offering or in connection with your payment method as being the place of supply for sales tax and income tax purposes or as being the place of supply for VAT purposes where you have established your business.

6. Temporary Suspension.

6.1 Generally. We may suspend your use of the Service Offering if we reasonably determine: (a) payment for the Service Offering is not received within 30 days from the date on which payment is due; (b) you are, or your use of the Service Offering is, in breach of this Agreement; (c) you fail to address our request to take action as specified in Section 3.3; (d) your use of the Service Offering poses a security risk to the Service Offering or other users of the Service Offering; or (e) suspension is required pursuant to our receipt of a subpoena, court order, or other request by a law enforcement agency. We will give you notice before we suspend, **subject to** applicable law, **and unless** we reasonably determine that **providing the notice presents** risk of harm to the Service Offering or any person or property.

6.2 Effect of Suspension. You will remain responsible for all fees incurred before or during any suspension. You will not be entitled to any service credits under any applicable Service Level Agreement that you might have otherwise accrued during the period of suspension.

7. Term and Termination.

7.1 Term of Agreement. This Agreement will be in effect until it is terminated as permitted herein or under the Service Description. For Subscription-based Service Offerings, the subscription will automatically renew as specified in the Service Description, unless terminated as permitted therein.

7.2 Termination for Cause. We may terminate this Agreement effective immediately upon sending you an email notice if you: (a) breach any provision of Sections 3.1 or 3.2; (b) do not resolve the underlying cause resulting in a suspension of your account pursuant to Section 6.1 (other than suspension due to a subpoena, court order, or other request by a law enforcement agency) within 10 days after your account is suspended; (c) commit a material breach of this Agreement that cannot be cured; or (d) terminate or suspend your business.

7.3 Termination for Insolvency. We may terminate this Agreement effective immediately upon sending you an email notice if you: (a) become insolvent, admit in writing your inability to pay your debts as they mature, or make an assignment for the benefit of creditors; or (b) become subject to control of a trustee, receiver or similar authority or any bankruptcy or insolvency proceeding.

7.4 Effect of Termination. Upon the effective date of termination of this Agreement for any reason: (a) all rights granted to you under this Agreement, including your ability to access the Service Offering, will immediately terminate; and (b) you must promptly discontinue all use of the Service Offering and delete or destroy any of our Confidential Information. Deletion and retrieval of Your Content will be handled as set forth in the Privacy Addendum. Section 1.6 (Open Source Software), 3 (Acceptable Use), 4 (IP Ownership), 5 (Orders, Delivery, Payment and Taxes), 7 (Term and Termination), 9 (Disclaimer), 11 (Limitation of Liability), 12 (Confidential Information), 13 (General), 14 (Definitions), 15 (Provisions for Specific Data Centers), and the Privacy Addendum will survive the termination of this Agreement. Termination of your use of the Service Offering (except to the extent that the termination is permitted under Sections 10.3 and 13.3 of this Agreement or Section 3.6 of the Service Description) will not entitle you to any refunds, credits, or exchanges, and you will be liable for all usage and other fees incurred up to the termination effective date, including any monthly billing fees for the remaining term of a Subscription-based Service Offering after the termination effective date.

8. Support and Subscription Services. When applicable, and subject to the terms of this Agreement, we will provide support for the Service Offering in accordance with the terms specified in the applicable Support Policy. We will not provide support to any end users of Your Content.

9. Disclaimer. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, WE AND OUR LICENSORS AND SERVICE PROVIDERS DISCLAIM ALL WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, SATSIFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE, RELATING TO THE SERVICE OFFERING OR ANY MATERIALS OR SERVICES PROVIDED TO YOU UNDER THIS AGREEMENT. WE AND OUR LICENSORS AND SERVICE PROVIDERS DO NOT WARRANT THAT THE SERVICE OFFERING WILL BE UNINTERRUPTED OR FREE FROM DEFECTS, OR THAT THE SERVICE OFFERING WILL MEET (OR IS DESIGNED TO MEET) YOUR BUSINESS REQUIREMENTS.

10. Indemnification.

10.1 Indemnification by You. You will defend and indemnify us against any third party claim arising from or relating to: (a) Your Content; (b) any infringement or misappropriation of any Intellectual Property Rights by you, Users or your suppliers in connection with your use of the Service Offering; (c) any violation of law by you or Users in connection with use of the Service Offering; (d) your or Users' use of the Service Offering in violation of this Agreement, or (e) your or Users' use of any Third Party Content. We will (1) provide you with notice of the claim within a reasonable period of time after learning of the claim; and (2) reasonably cooperate in response to your requests for assistance. You may not settle or compromise any indemnified claim without our prior written consent.

10.2 Defense and Indemnification. Subject to the remainder of this Section 10, we will defend you against an Infringement Claim and indemnify you from the resulting costs and damages finally awarded against you to that third party by a court of competent jurisdiction or agreed to in settlement. You will (a) provide us with notice of any Infringement Claim within a reasonable period of time after learning of it; (b) allow us sole control over the claim's defense and settlement; and (c) reasonably cooperate in response to our requests for assistance. You may not settle or compromise any Infringement Claim without our prior written consent.

10.3 Remedies. If the Service Offering becomes, or in our opinion is likely to become, the subject of an Infringement Claim, we will at our option and expense: (a) procure the rights necessary for you to keep using the Service Offering; (b) modify or replace the Service Offering to make it non-infringing; or (c) terminate this Agreement and refund any pre-paid fees for a Subscription-based Service Offering pro-rated for its remaining term.

10.4 Exclusions. We will have no obligation under this Section 10 or otherwise with respect to any claim based on: (a) a combination of VMware Software with non-VMware products or content, including Your Content; (b) use of the Service Offering for a purpose or in a manner not specified in this Agreement or the Service Description; (c) any modification to the Service Offering made without our express written approval; or (d) any Service Offering provided on a no-charge basis. This Section 10 states your exclusive remedy for any infringement claims.

11. Limitation of Liability.

11.1 Generally. TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT WILL WE BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE OF THE SERVICE OFFERING OR YOUR CONTENT, LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY OR OTHERWISE. IN ANY EVENT, OUR LIABILITY UNDER THIS AGREEMENT WILL NOT, REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE, EXCEED THE GREATER OF: (A) THE AGGREGATE FEES PAID OR PAYABLE TO US FOR YOUR ACCESS TO AND USE OF THE SERVICE OFFERING IN THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO THE CLAIM, OR (B) FIVE THOUSAND U.S. DOLLARS ($5,000 USD) (OR THE EQUIVALENT IN LOCAL CURRENCY), REGARDLESS OF WHETHER WE OR OUR LICENSORS OR SERVICE PROVIDERS HAVE BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE. THE LIMITATIONS OF LIABILITY IN THIS SECTION 11.1 WILL NOT APPLY TO (A) VMWARE'S INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT OR (B) ANY LIABILITY WHICH MAY NOT BE EXCLUDED BY APPLICABLE LAW.

11.2 Further Limitations. Our licensors and service providers will have no liability of any kind under this Agreement. You may not bring a claim under this Agreement more than eighteen (18) months after the cause of action arises.

12. Confidential Information.

12.1 Protection. A party may use Confidential Information of the other party solely to exercise its rights and perform its obligations under this Agreement or as otherwise permitted under this Agreement. Each party will disclose the Confidential Information of the other party only to the employees, service providers or contractors of the recipient party who have a need to know the Confidential Information for purposes of this Agreement and who are under a duty of confidentiality no less restrictive than each party's duty under this Agreement. Each party will use reasonable care to protect the confidentiality of the other party's Confidential Information.

12.2 Exceptions. The recipient's obligations under Section 12.1 with respect to any Confidential Information will terminate if the recipient can show by written records that the information: (a) was already rightfully known to the recipient at the time of disclosure by the other party; (b) was disclosed to the recipient by a third party who had the right to make the disclosure without any confidentiality restrictions; (c) is, or through no fault of the recipient has become, generally available to the public; or (d) was independently developed by the recipient without access to, or use of, discloser's Confidential Information. The recipient may disclose Confidential Information to the extent the disclosure is required by law or regulation or the listing rules of any stock exchange. The recipient will provide the other party notice, when practicable, and will take reasonable steps to contest and limit the scope of any required disclosure.

13. General.

13.1 Assignment. You may not assign or transfer this Agreement, in whole or in part, by operation of law or otherwise, without our prior written consent. Any attempted assignment or transfer without that consent will be void. Subject to these limits, this Agreement will bind and inure to the benefit of the parties and their respective successors and assigns.

13.2 Notices. Any notice delivered by us to you under this Agreement will be delivered by email to the email address associated with your account or by posting on either the Service Offering Portal or the My VMware Portal, except as otherwise set forth in this Agreement. You will direct legal notices or other correspondence to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America, Attention: Legal Department.

13.3 Modifications. We may change periodically the Service Offering, the terms of your access to the Service Offering, this Agreement, the Service Description, the Privacy Addendum, the Service Level Agreement, or the Support Policy. It is your responsibility to regularly check the Service Offering and My VMware portals for updates. We will notify you of any material, detrimental change to this Agreement, the Service Description, the Privacy Addendum, the Service Level Agreement, or the Support Policy. In the case of a material, detrimental change to the Service Level Agreement, we will notify you at least 90 days prior to the effective date of the change. The modified Agreement, Service Description, Privacy Addendum, Service Level Agreement, or Support Policy, as applicable, will become effective as of the date stated in that notification. If we make a material, detrimental change to the Service Offering (other than the termination or modification of any beta feature or functionality), this Agreement, the Service Description, the Privacy Addendum, the Service Level Agreement, or the Support Policy, then you may terminate this Agreement no later than 30 days after the effective date of the change. If you terminate this Agreement pursuant to this Section 13.3, the termination will be effective as of the date we receive your notification, unless you state in your notification an effective date that is later but within 45 days after we receive your notification. If you terminate a Subscription-based Service Offering, we will refund any prepaid fees, pro-rated for the remainder of the term, and less any discounts that would not be earned as of the effective date of the termination. Your continued use of the Service Offering after the effective date of any modification to the Agreement, the Service Description, the Privacy Addendum, the Service Level Agreement, or the Support Policy will be deemed acceptance of the modified terms, as applicable.

13.4 Waiver. The waiver of a breach of any provision of this Agreement will not constitute a waiver of any other provision or any later breach.

13.5 Severability. If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions of this Agreement will remain in force.

13.6 Compliance with Laws; Export Control. Each party will comply with all laws applicable to the actions contemplated by this Agreement. You acknowledge that the Service Offering is of United States origin, is provided subject to the U.S. Export Administration Regulations (including "deemed export" and "deemed re-export" regulations), and may be subject to the export control laws of the applicable country. You represent and warrant that (a) you are not, and are not acting on behalf of, (1) any person who is a citizen, national, or resident of, or who is controlled by, the government of any country to which the United States has prohibited export transactions; (2) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List, or any similar designated persons list published for the jurisdiction in which the data center you choose for the Service Offering is located; (b) you will not permit the Service Offering to be used for any purposes prohibited by law, including any prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons; (c) Your Content will not be classified or listed on the United States Munitions list or similar list published for the jurisdiction in which the data center you choose for the Service Offering is located, or contain defense articles, defense services or ITAR-related data; (d) Your Content will not require an export license and is not restricted under applicable export control laws from export to any country where VMware or VMware's service providers maintain facilities or personnel; and (e) you are not subject, either directly or indirectly, to any order issued by any agency of the United States government, revoking or denying, in whole or in part, your United States export privileges. You will notify VMware immediately if you become subject to any such order.

13.7 Government Regulations. For purposes of sales to government entities in the U.S.: The Service Offering and its documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFARS Section 227.7202 and FAR Paragraph 12.212(b), as applicable. Any use, modification, reproduction, release, performing, displaying or disclosing of the Service Offering and documentation by or on

behalf of the U.S. Government will be governed solely by the terms and conditions of this Agreement.

13.8 Force Majeure. We will not be liable for any delay or failure to perform any obligations under this Agreement due to any cause beyond our reasonable control, including acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications or other utility failures, earthquakes, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism or war.

13.9 Construction. The headings of sections of this Agreement are for convenience and are not for use in interpreting this Agreement. As used in this Agreement, the word 'including' means "including but not limited to."

13.10 Governing Law. This Agreement is governed by the laws of the State of California, United States of America (excluding its conflict of law rules), except as follows: for Service Offering purchases where you choose a data center that is outside the United States of America, the governing laws are those of the country in which the data center is located (excluding its conflict of law rules). The United Nations Convention for the International Sale of Goods does not apply. This Agreement does not affect your statutory rights that cannot be waived or changed by contract.

13.11 Third Party Rights. Other than as expressly provided in this Agreement, this Agreement does not create any rights for any person who is not a party to it, and no person who is not a party to this Agreement may enforce any of its terms or rely on any exclusion or limitation contained in it.

13.12 Order of Precedence. The terms of this Agreement will supersede and control over any conflicting or additional terms and conditions of any other purchasing related document issued by you.

13.13 Entire Agreement. This Agreement, as it may be revised by us, is the entire agreement of the parties regarding its subject matter. This Agreement supersedes all prior or contemporaneous communications, understandings and agreements, whether written or oral, between the parties regarding its subject matter.

14. Definitions.

14.1 " **Confidential Information**" means non-public technical, business or other information or materials disclosed or otherwise made available by one party in connection with the Service Offering that are in tangible form and labeled "confidential" or the like, or are provided under circumstances reasonably indicating their confidentiality. Our Confidential Information includes: (1) Login Credentials; and (2) any information or materials relating to the Service Offering.

14.2 " **Infringement Claim**" means any third party claim that any VMware Software used to provide the Service Offering infringes any patent, trademark or copyright of the third party, or misappropriates a trade secret (but only to the extent that the misappropriation is not a result of your actions) under the laws of: (a) the United States; (b) Canada; (c) the European Economic Area member states; (d) Australia; (e) New Zealand; (f) Japan; or (g) the People's Republic of China, to the extent that those countries are part of your places of use of the Service Offering.

14.3 " **Intellectual Property Rights**" means all worldwide intellectual property rights, including copyrights, trademarks, service marks, trade secrets, patents, patent applications, and moral rights, whether registered or unregistered.

14.4 " **Login Credentials**" mean any passwords, authentication keys or security credentials that enable your access to and management of the Service Offering.

14.5 " **OnDemand-based Service Offering**" means a Service Offering for which you pay for actual usage in arrears on a periodic basis, as specified in your Order.

14.6 " **Order**" means the internet order page, or other ordering document, that specifies your purchase of the Service Offering.

14.7 " **Privacy Addendum**" means the then-current version of the Service Offering Data Privacy Addendum document available at http://www.vmware.com/download/eula/vrealize-air-data-privacy-addendum (/download/eula/vrealize-air-data-privacy-addendum.html).

14.8 " **Service Description**" means the then-current version of the Service Offering Service Description document available at https://www.vmware.com/files/pdf/support/vrealize-air-service-description.pdf (/content/dam/digitalmarketing/vmware/en/pdf/products/support/vrealize-air-service-description.pdf), which contains technical and other information.

14.9 " **Service Level Agreement**" means the then-current version of the Service Offering Service Level Agreement document available at http://www.vmware.com/download/eula/vrealize-air-service-level-agreement (/download/eula/vrealize-air-service-level-agreement.html).

14.10 " **Subscription-based Service Offering**" means a Service Offering for which you pay in advance for use of the Service Offering for a fixed period as specified in your Order. A Subscription-based Service Offering may also include optional services (e.g., add-ons) and metered usage components.

14.11 " **Support Policy**" means the then-current version of the Service Offering Support Policy document available at https://www.vmware.com/support/policies/saas-support.html (/support/policies/saas-support.html), which we may modify from time to time.

14.12 " **Third Party Content**" means third party data, service, content, software or applications, including open source software.

14.13 " **User**" means any person that accesses Your Content or uses the Service Offering under your Login Credentials.

14.14 " **VMware Software**" means the software programs listed in our commercial price list.

14.15 " **Your Content**" means any and all applications, services, files, information, data or other content uploaded to or published or displayed through the Service Offering by you, Users, or us (acting upon your instructions as part of a service).

15. Provisions for Specific Data Centers. For Service Offering purchases where you choose a data center located in the countries listed below, the following provisions replace or supplement the referenced sections of this Agreement, as noted.

15.1 Australian Data Center:
15.1.1 Supplement Section 9 titled "Disclaimer" with the following additional paragraph:
"Nothing in this Agreement (including this Section 9 and Section 1.5) excludes, restricts or modifies any consumer guarantee, right or remedy conferred on you by the Australian Consumer Law or any other applicable law that cannot be excluded, restricted or modified by agreement. Subject to the preceding sentence, any condition, warranty, guarantee, right or liability which would otherwise be implied in this Agreement or imposed by law is excluded. VMware's liability for any breach of any consumer guarantee, right or remedy conferred by the Australian Consumer Law which cannot be excluded is limited, at VMware's option, to supplying the applicable service again or to the payment of the cost of having that service provided again."

15.1.2 Replace the first sentence of Section 13.10 titled "Governing Law" with the following:
"This Agreement is governed by the laws of New South Wales, Australia, without regard to conflict of law principles."

15.2 German Data Center:
15.2.1 Replace the last sentence of Section 1.4 titled "Additional Terms; Third Party Content" with the following sentence:
"Except as permitted under Sections 6 and 7, we will only suspend or terminate Third Party Content during a subscription term with thirty (30) days prior notice, in which case we will provide a pro-rata refund of any pre-payments (if any) made for such suspended or terminated Third Party Content."

15.2.2 In Section 1.5 titled "Evaluation and Beta Use", remove the period at the end of the third sentence which reads "[...] (b) "AS IS", excluding any Service Level Agreement, and without indemnification or warranty or condition of any kind." And add the following to the end of the third sentence:
", except insofar as defects have been fraudulently concealed by us."

15.2.3 Replace Section 7.3 titled "Termination for Insolvency" with the following:
" 7.3 [Reserved]"

15.2.4 Replace Section 9 titled "Disclaimer" with the following:
" 9. Limited Warranty.

9.1 Qualities. During the Service Offering term, the Service Offering will substantially conform to the applicable Service Description unless otherwise stated herein. We do not commit that the Service Offering will be uninterrupted or that the Service Offering does fulfill any merchantability or fitness for a particular purpose, or will meet (or is designed to meet) your business requirements, unless stated otherwise in the applicable Service Description or individually agreed between the parties.

9.2 Warranty. We will correct any defect in the aforementioned qualities of the Service Offering reported to us by you in writing. If we are unable to correct the defect, we will refund an appropriate portion of the fees paid by you with respect to the affected portion of the affected Service Offering.

9.3 Any Service Credits (as set forth in the Service Level Agreement), will be set off against any refund for breach of warranty, if and to the extent such Service Credits are provided for the same event that entitles you to a refund for breach of warranty.

9.4 Subject to Section 11, the remedies in Section 9.2 are your sole and exclusive remedies for breach of warranty and our sole and exclusive liability for breach of warranty."

15.2.5 Replace Section 11 titled "Limitation of Liability" with the following:
" 11.1 Limitation. Our liability for a claim of any nature arising out of this Agreement, regardless of whether the claim is based in contract, tort, strict liability, or otherwise,

11.1.1 will be limited to damages that are foreseeable and typical for this type of contract ("vertragstypische und vorhersehbare Schäden") arising from a slight negligent breach of a material contractual obligation ("Kardinalpflicht", i.e. an obligation the fulfillment of which is essential to enable the proper performance of the contract, and on which fulfillment you may rely on); and

11.1.2 will not exceed per damage event (i) EUR 250.000 (Two Hundred Fifty Thousand Euro), or (ii) if the aggregate fees paid or payable to us for your access to and use of the Service Offering in the twelve (12) months prior to the event giving rise to your claim are higher, then those fees for the specific Service Offering given rise to such claim (subject to the limit set forth in Section 11.1.3 below).

11.1.3 In no event will our total and cumulative liability for all claims arising out of this Agreement exceed EUR 500.000 (Five Hundred Thousand Euro).

11.2 Disclaimer of Liability. In case of slight negligence, we will not be liable for any indirect or consequential damages (including, but not limited to any loss of profits, business opportunity, revenue or goodwill), even if we have been advised as to the possibility of such damages.

11.3 Further Limitations. Our licensors and service providers will have no liability of any kind under this Agreement. You may not bring a claim under this Agreement more than eighteen (18) months after the cause of action arises.

11.4 Exceptions. Nothing in this Agreement will limit or exclude our liability for death or personal injury, for intentional act or gross negligence, fraudulent misrepresentation, fraudulent concealment of a defect, mandatory liability under the German Product Liability Act (Produkthaftungsgesetz), or liability for any damages resulting from a breach of a given guarantee."

15.3 United Kingdom Data Center:
15.3.1 Replace the last sentence in Section 1.4 titled "Additional Terms; Third Party Content" with the following sentence:
"Except as permitted under Sections 6 and 7, we will only suspend or terminate Third Party Content during a subscription term with thirty (30) days prior notice, in which case we will provide a pro-rata refund of any pre-payments (if any) made for such suspended or terminated Third Party Content."

15.3.2 Supplement Section 7.3 titled "Termination for Insolvency" with the following:
"(c) if you are deemed unable to pay your debts within the meaning of Section 123 of the Insolvency Act of 1986; or (d) suffer or undergo any similar or analogous suspension or proceeding in any jurisdiction."

15.3.3 Replace the last sentence of Section 10.4 "[Indemnification] Exclusions" with the following:
"This Section 10 states your exclusive remedy for any infringement claims or actions arising out of or related to any infringement claims."

15.3.4 Replace the last sentence of Section 11.1 titled "Generally" with the following:
"THE LIMITATIONS OF LIABILITY IN THIS SECTION 11.1 WILL NOT APPLY TO VMWARE'S INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT. NOTHING IN THIS AGREEMENT SHALL LIMIT OR EXCLUDE ANY PARTY'S LIABILITY FOR DEATH OR PERSONAL INJURY, FOR FRAUDULENT MISREPRESENTATION, OR FOR ANY OTHER LIABILITY WHICH MAY NOT BE LIMITED OR EXCLUDED BY APPLICABLE LAW."

15.3.5 Supplement Section 12.2 titled "[Confidential Information] Exceptions" with the following:
"Breach of this Section 12 by the recipient party may cause the disclosing party substantial harm for which monetary damages are an insufficient remedy. Accordingly, each party agrees that the other party may apply for injunctive relief in respect of any threatened or actual breach of this Section 12."

15.3.6 Any reference to "warranty or condition" is deemed to refer to "warranty, condition or other terms", any reference to "warranties and conditions" is deemed to refer to "warranties, conditions, and other terms" and any reference to "warranties or conditions" is deemed to refer to "warranties, conditions or other terms."

Related Resources

Terms of Service (/download/eula/vrealize-air-terms-of-service.html)
Service Description PDF (/content/dam/digitalmarketing/vmware/en/pdf/products/support/vrealize-air-service-description.pdf)
Service Level Agreement (/download/eula/vrealize-air-service-level-agreement.html)
Data Privacy Addendum (/content/dam/digitalmarketing/vmware/en/pdf/products/vmware-data-privacy-addendum.pdf)
Privacy Policy (/help/privacy.html)

© 2017 VMware, Inc

(/)

(/)

(/)

(/)

(/)

VMware Horizon® Air™ Desktops and Horizon Air Hybrid-Mode

(/)

TERMS OF SERVICE

Last updated: December 1, 2016

By accessing the VMware hosted service specified in your Order (the "**Service Offering**"), you agree to be bound by these terms of service between you and VMware ("**Agreement**"). This Agreement also includes the applicable Service Description, Privacy Addendum, Third Party Terms, Support Policy, and Service Level Agreement. If you do not agree to this Agreement, you must not access the Service Offering. "**You**" means you individually or the entity that you represent. If you are entering into this Agreement for an entity, you represent to us that you have legal authority to bind that entity. "**VMware**," "**we**," or "**us**" means VMware, Inc., a Delaware corporation, to the extent that you purchase the Service Offering in the United States, and VMware International Limited, a company organized and existing under the laws of Ireland, to the extent that you purchase the Service Offering elsewhere. Capitalized terms used in this Agreement are defined throughout this Agreement and in Section 14.

Related Resources

- Service Level Agreement - Horizon Air Desktops (/download/eula/horizon-air-service-license-agreement.html)
- Service Level Agreement - Horizon Air Hybrid Mode (/download/eula/horizon-air-hybrid-mode-service-level-agreement.html)
- Service Description - Horizon Air Desktops (/content/dam/digitalmarketing/vmware/en/pdf/support/vmware-horizon-air-service-description.pdf)
- Service Description - Horizon Air Hybrid Mode (/content/dam/digitalmarketing/vmware/en/pdf/support/horizon-air-hybrid-mode-service-description.pdf)
- Data Privacy Addendum (/content/dam/digitalmarketing/vmware/en/pdf/products/vmware-data-privacy-addendum.pdf)
- Third Party Terms (/content/dam/digitalmarketing/vmware/en/pdf/support/vmware-horizon-air-third-party-terms.pdf)
- Support Policy (/support/policies/saas-support.html)

1. The Service Offering.

1.1 Generally. This Agreement governs your access to and use of the Service Offering. We may deliver the Service Offering to you with the assistance of our affiliates, licensors and service providers. You will comply with all laws, rules and regulations applicable to your use of the Service Offering. You also will comply with the applicable Third Party Terms, Service Description, Privacy Addendum, and Support Policy. If you access the Service Offering, or any of its features or functionality, on an evaluation or beta basis, please see Section 1.5 for other terms that apply to you.

1.2 Access to the Service Offering. You may access and use the Service Offering solely for your own benefit and only in accordance with this Agreement. To access the Service Offering, you must register for the Service Offering and set up an authorized account with Login Credentials. You may monitor and manage your Service Offering account via the My VMware Portal available at www.vmware.com/accounts (http://www.vmware.com/accounts) and through the Service Offering Portal made available to you. You must keep confidential your Login Credentials. If you set up an authorized account for an organization, you must require that all authorized Users of that account (including anyone providing services to you) keep confidential their Login Credentials. You must keep your registration information accurate, complete and current for as long as you use the Service Offering. You are responsible for any use that occurs under your Login Credentials, including any activities by you or your employees, contractors or agents. If you believe an unauthorized person has gained access to your Login Credentials, you must notify us as soon as possible by submitting a Severity 1 Service Request (see the applicable Support Policy).

1.3 Verifying Compliance; Cooperation. We have the right to verify your compliance with this Agreement. If we seek to verify that compliance, you will provide information or other materials reasonably requested by us to assist in the verification. We monitor the overall performance and stability of the infrastructure of the Service Offering. You may not block or interfere with that monitoring. If we reasonably believe a problem with the Service Offering may be attributable to Your Content or your use of the Service Offering, you will cooperate with us to identify the source of and resolve that problem.

1.4 Third Party Content. As part of your use of the Service Offering, you may receive access to Third Party Content, which is subject to separate terms. If so, those separate terms will prevail over this Agreement as to your use of the Third Party Content. Third Party Content is available "AS IS" without indemnification, support (unless otherwise noted in the Third Party Terms), or warranty or condition of any kind You are responsible for reviewing, accepting, and complying with any third party terms of use or other restrictions applicable to the Third Party Content. Those terms will be available to you in the Third Party Terms or through a notification within the Service Offering. We reserve the right to suspend or terminate the Third Party Content at any time. We will use commercially reasonable efforts to provide reasonable notice of that suspension or termination.

1.5 Evaluation and Beta Use. If you access the Service Offering, or a feature or functionality of the Service Offering, on an evaluation or beta basis (either referred to as the "Evaluation Service"), then you may use the Evaluation Service only for evaluation purposes and for the period we specify. You must not use the Evaluation Service for any production computing activity. Notwithstanding any other provision of this Agreement, we provide the Evaluation Service (a) free of charge and without support; and (b) "AS IS", excluding any Service Level Agreement, and without indemnification or

warranty or condition of any kind. Also, certain features or services described in the Service Description may not be available for the Evaluation Service. You will not have access to Your Content or the Evaluation Service after it terminates, and the features and functionality of the Evaluation Service do not constitute an implied commitment to offer them to you or anyone as part of the Service Offering on a generally available basis.

(/)

1.6 Open Source Software. You may receive open source software when you use the Service Offering. Any open source software distributed to you is made available under the applicable open source license, which can be found at: http://www.vmware.com/download/open_source.html (/download/open_source.html). You may obtain a copy of these licenses and any source code (and modifications) that we are required to make available under these licenses (the "**Source Files**") at http://www.vmware.com/download/open_source.html (/download/open_source.html) or by sending a written request, with your name and address, to: VMware, Inc., 3401 Hillview Avenue, Palo Alto, CA 94304, United States of America. All written requests must clearly specify: Open Source Files Request, Attention: General Counsel. This offer to obtain a copy of the Source Files is valid for three years from the date you last received open source software as part of the Service Offering.

2. Data Protection and Security.

2.1 Data Protection. We will process personal data contained in Your Content, and maintain appropriate technical and organizational measures (administrative, physical and technical safeguards), as set forth in the Privacy Addendum.

2.2 Your Content; Security. You are solely responsible for Your Content. Except as provided by the Privacy Addendum, You are responsible for protecting the security of Your Content, including any access to Your Content that you might provide to your employees, customers or other third parties, and when it is in transit to and from the Service Offering. The Service Offering provides you with certain software and functionality to help you protect Your Content from unauthorized access. You must take and maintain appropriate steps regarding the security, protection and backup of Your Content, which might include the use of encryption technology to protect Your Content from unauthorized access. You are responsible for providing any necessary notices to Users and for obtaining any legally-required consents from Users concerning their use of the Service Offering. You are responsible for complying with any laws or regulations that might apply to Your Content. You are responsible for any losses or other consequences arising from your failure to encrypt or back up Your Content.

3. Acceptable Use.

3.1 General Restrictions. You and any Users accessing the Service Offering through you may not: (a) resell or sublicense the Service Offering; or (b) use or access the Service Offering: (i) in a way prohibited by law, regulation, governmental order or decree; (ii) to violate any rights of others; (iii) to try to gain unauthorized access to, test the vulnerability of, or disrupt the Service Offering or any other service, device, data, account or network; (iv) to spam or distribute malware; (v) in a way that could harm the Service Offering or impair anyone else's use of it; (vi) in a way intended to work around the Service Offering's technical limitations, recurring fees or usage limits; or (vii) in any application or situation where failure of the Service Offering could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage. You must ensure that your Users comply with the terms of this Agreement, and you agree that if you become aware of any violation by one of your Users, you will immediately terminate that User's access to Your Content. If we have reason to believe that you or your Users have breached this Agreement, we or our designated representative may review your use of the Service Offering, including your account, Your Content, and your records, to verify your compliance with this Agreement.

3.2 Content Restrictions. You will take steps to ensure that any User does not post content that: (a) may create a risk of harm, loss, physical or mental injury, emotional distress, death, disability, disfigurement, or physical or mental illness to anyone; (b) may create a risk of any other loss or damage to any person or property; (c) may constitute or contribute to a crime or tort; (d) contains any information or content that is illegal, unlawful, harmful, abusive, pornographic, racially or ethnically offensive, defamatory, infringing, invasive of personal privacy or publicity rights, harassing, humiliating to other people (publicly or otherwise), libelous, threatening, or otherwise objectionable; or (e) contains any information or content that you do not have a right to make available under any law or under contractual or fiduciary relationships. You are responsible for any software, product or service that a third party licenses, sells or makes available to you that you install or use with the Service Offering. Your use of that software, product or service is governed by separate terms between you and that third party. We are not a party to and are not bound by any of those separate terms. You represent and warrant that Your Content does not and will not violate any third-party rights, including any Intellectual Property Rights, and rights of publicity and privacy. You will ensure that your use of the Service Offering complies at all times with your privacy policies and all applicable laws and regulations, including any encryption requirements.

3.3 Violations of Acceptable Use. If you become aware that any of Your Content or any User's access to or use of Your Content violates Sections 3.1 or 3.2, you will take immediate action to remove the applicable part of Your Content or suspend the User's access. We may also ask you to take action within a certain time period, and if you fail to comply with the request, we may suspend your account pursuant to Section 6.

3.4 Notification of Infringement Concerns. If you believe that your copyrighted work has been copied and is accessible on the Service Offering in a way that constitutes copyright infringement, please send a notice to us as provided in Section 8 of the Community Terms of Use available at http://www.vmware.com/community_terms.html (http://www.vmware.com/community_terms.html).

4. IP Ownership.

4.1 Ownership of Service Offering. We and our licensors own and retain all right, title and interest in and to the Service Offering and any related VMware Software, including all improvements, enhancements, modifications and derivative works thereof, and all Intellectual Property Rights therein. This includes any information that we collect and analyze in connection with the Service Offering, such as usage patterns, user feedback and other information to improve and evolve our software products and services offerings. Your rights to use the Service Offering are limited to those expressly granted in this Agreement. No other rights with respect to the Service Offering, any related VMware Software, or any related Intellectual Property Rights are implied.

4.2 Ownership of Your Content. You and your authorized Users retain all right, title and interest in and to Your Content and all Intellectual Property Rights therein. Our rights to access and use Your Content are limited to those expressly granted in this Agreement. No other rights with respect to Your Content or any related Intellectual Property Rights are implied.

4.3. Feedback. We will be free to use for any purpose any feedback (such as comments or suggestions) that you provide to us regarding the Service Offering. You hereby grant to us a non-exclusive, perpetual, irrevocable, royalty-free, transferable, worldwide right and license, with the right to sublicense, to use, reproduce, perform, display, disclose, distribute, modify, prepare derivative works of and otherwise exploit the feedback without restriction in any manner now known or in the future conceived and to make, use, sell, offer to sell, import and export any product or service that incorporates the feedback.

5. Orders, Delivery, Payment, and Taxes.

5.1 Orders Generally. All Orders issued to VMware are subject to the terms of this Agreement and are not binding until accepted by VMware. We are not required to provide any Service Offering to you until you provide all information we require for processing your Order. Your Order will be deemed accepted when we authorize the purchased Service Offering for your Login Credentials.

5.2 Delivery. When VMware accepts your Order for the Service Offering, we will deliver the corresponding Login Credentials to you by email to the address associated with your account. If VMware ships a physical object in connection with an add-on feature of the Service Offering, shipping and delivery terms are Ex Works VMware's regional fulfillment facility (INCOTERMS 2010).

5.3 Direct Orders. This Section 5.3 applies only to Orders and purchases you make directly with VMware. A VMware authorized reseller might specify similar terms when you make an Order or purchase through that reseller.

5.3.1 Purchase Orders. For Subscription-based Service Offering orders placed directly with VMware, you must issue a purchase order to VMware for the initial Service Offering order, but a purchase order is not required for us to invoice you for the monthly billings that occur after the initial Order billing.

5.3.2 Invoicing and Payment. We will bill you as specified in the Service Description. You will pay all fees for use of the Service Offering in the amount and currency specified in your invoice by one of the payment methods that we support as specified in the Service Description, and in any event no later than 30 days after the date of the invoice. For an OnDemand-based Service Offering, you will pay in arrears on a monthly basis the applicable fees based on your actual metered usage of the Service Offering. For a Subscription-based Service Offering, you will pay in advance the applicable fees for the monthly or prepaid charges due, and you will pay in arrears the initial monthly fees and for any metered usage components consumed. The applicable fees for the Service Offering will be governed by the then-current applicable price list at the time of invoicing. We may increase or add new fees for the Service Offering by notifying you at least 30 days in advance.

5.3.3 Taxes. Service Offering fees are exclusive of Taxes. "Taxes" means any sales, VAT, GST (Goods and Services Tax), use, gross receipts, business and occupation, and other taxes (other than taxes on our income), export and import fees, customs duties and similar charges imposed by any government or other authority. You shall pay or reimburse us for all Taxes arising out of the transactions contemplated by this Agreement. If you are required to pay or withhold any Tax for payments due under this Agreement, you shall gross up your payments to us so that we receive sums due in full and free of any deductions. If you are required to pay any Tax to a taxing authority, you will also provide documentation to us showing that you paid those Taxes to the relevant taxing authority. You hereby confirm that we can rely on the name and address you provide to us when you agree to the Service Offering or in connection with your payment method as being the place of supply for sales tax and income tax purposes or as being the place of supply for VAT purposes where you have established your business.

6. Temporary Suspension.

6.1 Generally. We may suspend your use of the Service Offering if we reasonably determine: (a) payment for the Service Offering is not received within 30 days from the date on which payment is due; (b) you are, or your use of the Service Offering is, in breach of this Agreement; (c) you fail to address our request to take action as specified in Section 3.3; (d) your use of the Service Offering poses a security risk to the Service Offering or other users of the Service Offering; or (e) suspension is required pursuant to our receipt of a subpoena, court order, or other request by a law enforcement agency. We will give you notice before we suspend, **subject to** applicable law, **and unless** we reasonably determine that **providing the notice presents** risk of harm to the Service Offering or any person or property.

6.2 Effect of Suspension. You will remain responsible for all fees incurred before or during any suspension. You will not be entitled to any service credits under any applicable Service Level Agreement that you might have otherwise accrued during the period of suspension.

7. Term and Termination.

7.1 Term of Agreement. This Agreement will be in effect until it is terminated as permitted herein or under the Service Description. For Subscription-based Service Offerings, the subscription will automatically renew as specified in the Service Description, unless terminated as permitted therein.

7.2 Termination for Cause. We may terminate this Agreement effective immediately upon sending you an email notice if you: (a) breach any provision of Sections 3.1 or 3.2; (b) do not resolve the underlying cause resulting in a suspension of your account pursuant to Section 6.1 (other than suspension due to a subpoena, court order, or other request by a law enforcement agency) within 10 days after your account is suspended; (c) commit a material breach of this Agreement that cannot be cured; or (d) terminate or suspend your business.

7.3 Termination for Insolvency. We may terminate this Agreement effective immediately upon sending you an email notice if you: (a) become insolvent, admit in writing your inability to pay your debts as they mature, or make an assignment for the benefit of creditors; or (b) become subject to control of a trustee, receiver or similar authority or any bankruptcy or insolvency proceeding.

7.4 Effect of Termination. Upon the effective date of termination of this Agreement for any reason: (a) all rights granted to you under this Agreement, including your ability to access the Service Offering, will immediately terminate; and (b) you must promptly discontinue all use of the Service Offering and delete or destroy any of our Confidential Information. Deletion and retrieval of Your Content will be handled as set forth in the Privacy Addendum. Section 1.6 (Open Source Software), 3 (Acceptable Use), 4 (IP Ownership), 5 (Orders, Delivery, Payment and Taxes), 7 (Term and Termination), 9 (Disclaimer), 11 (Limitation of Liability), 12 (Confidential Information), 13 (General), 14 (Definitions), 15 (Provisions for Specific Data Centers), and the Privacy Addendum will survive the termination of this Agreement. Termination of your use of the Service Offering (except to the extent that the

termination is permitted under Sections 10.3 and 13.3 of this Agreement or section 3.6 of the Service Description) will not entitle you to any refunds, credits, or exchanges, and you will be liable for all usage and charges incurred up to the termination effective date, including any monthly billing fees for the remaining term of a Subscription-based Service Offering after the termination effective date.

(/)

8. Support and Subscription Services. When applicable, and subject to the terms of this Agreement, we will provide support for the Service Offering in accordance with the terms specified in the applicable Support Policy. We will not provide support to any end users of Your Content.

9. Disclaimer. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, WE AND OUR LICENSORS AND SERVICE PROVIDERS DISCLAIM ALL WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, SATSIFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE, RELATING TO THE SERVICE OFFERING OR ANY MATERIALS OR SERVICES PROVIDED TO YOU UNDER THIS AGREEMENT. WE AND OUR LICENSORS AND SERVICE PROVIDERS DO NOT WARRANT THAT THE SERVICE OFFERING WILL BE UNINTERRUPTED OR FREE FROM DEFECTS, OR THAT THE SERVICE OFFERING WILL MEET (OR IS DESIGNED TO MEET) YOUR BUSINESS REQUIREMENTS.

10. Indemnification.

10.1 Indemnification by You. You will defend and indemnify us against any third party claim arising from or relating to: (a) Your Content; (b) any infringement or misappropriation of any Intellectual Property Rights by you, Users or your suppliers in connection with your use of the Service Offering; (c) any violation of law by you or Users in connection with use of the Service Offering; (d) your or Users' use of the Service Offering in violation of this Agreement, or (e) your or Users' use of any Third Party Content. We will (1) provide you with notice of the claim within a reasonable period of time after learning of the claim; and (2) reasonably cooperate in response to your requests for assistance. You may not settle or compromise any indemnified claim without our prior written consent.

10.2 Defense and Indemnification. Subject to the remainder of this Section 10, we will defend you against an Infringement Claim and indemnify you from the resulting costs and damages finally awarded against you to that third party by a court of competent jurisdiction or agreed to in settlement. You will (a) provide us with notice of any Infringement Claim within a reasonable period of time after learning of it; (b) allow us sole control over the claim's defense and settlement; and (c) reasonably cooperate in response to our requests for assistance. You may not settle or compromise any Infringement Claim without our prior written consent.

10.3 Remedies. If the Service Offering becomes, or in our opinion is likely to become, the subject of an Infringement Claim, we will at our option and expense: (a) procure the rights necessary for you to keep using the Service Offering; (b) modify or replace the Service Offering to make it non-infringing; or (c) terminate this Agreement and refund any pre-paid fees for a Subscription-based Service Offering pro-rated for its remaining term.

10.4 Exclusions. We will have no obligation under this Section 10 or otherwise with respect to any claim based on: (a) a combination of VMware Software with non-VMware products or content, including Your Content; (b) use of the Service Offering for a purpose or in a manner not specified in this Agreement or the Service Description; (c) any modification to the Service Offering made without our express written approval; or (d) any Service Offering provided on a no-charge basis. This Section 10 states your exclusive remedy for any infringement claims.

11. Limitation of Liability.

11.1 Generally. TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT WILL WE BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE OF THE SERVICE OFFERING OR YOUR CONTENT, LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY OR OTHERWISE. IN ANY EVENT, OUR LIABILITY UNDER THIS AGREEMENT WILL NOT, REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE, EXCEED THE GREATER OF: (A) THE AGGREGATE FEES PAID OR PAYABLE TO US FOR YOUR ACCESS TO AND USE OF THE SERVICE OFFERING IN THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO THE CLAIM, OR (B) FIVE THOUSAND U.S. DOLLARS ($5,000 USD) (OR THE EQUIVALENT IN LOCAL CURRENCY), REGARDLESS OF WHETHER WE OR OUR LICENSORS OR SERVICE PROVIDERS HAVE BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE. THE LIMITATIONS OF LIABILITY IN THIS SECTION 11.1 WILL NOT APPLY TO (A) VMWARE'S INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT OR (B) ANY LIABILITY WHICH MAY NOT BE EXCLUDED BY APPLICABLE LAW.

11.2 Further Limitations. Our licensors and service providers will have no liability of any kind under this Agreement. You may not bring a claim under this Agreement more than eighteen (18) months after the cause of action arises.

12. Confidential Information.

12.1 Protection. A party may use Confidential Information of the other party solely to exercise its rights and perform its obligations under this Agreement or as otherwise permitted under this Agreement. Each party will disclose the Confidential Information of the other party only to the employees, service providers or contractors of the recipient party who have a need to know the Confidential Information for purposes of this Agreement and who are under a duty of confidentiality no less restrictive than each party's duty under this Agreement. Each party will use reasonable care to protect the confidentiality of the other party's Confidential Information.

12.2 Exceptions. The recipient's obligations under Section 12.1 with respect to any Confidential Information will terminate if the recipient can show by written records that the information: (a) was already rightfully known to the recipient at the time of disclosure by the other party; (b) was disclosed to the recipient by a third party who had the right to make the disclosure without any confidentiality restrictions; (c) is, or through no fault of the recipient has become, generally available to the public; or (d) was independently developed by the recipient without access to, or use of, discloser's Confidential Information. The recipient may disclose Confidential Information to the extent the disclosure is required by law or regulation or the listing rules of any stock exchange. The recipient will provide the other party notice, when practicable, and will take reasonable steps to contest and limit the scope of any required disclosure.

13. General.

13.1 Assignment. You may not assign or transfer this Agreement, in whole or in part, by operation of law or otherwise, without our prior written consent. Any attempted assignment or transfer without that consent will be void. Subject to these limits, this Agreement will bind and inure to the benefit of the parties and their respective successors and assigns.

(/)

13.2 Notices. Any notice delivered by us to you under this Agreement will be delivered by email to the email address associated with your account or by posting on either the Service Offering Portal or the My VMware Portal, except as otherwise set forth in this Agreement. You will direct legal notices or other correspondence to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America, Attention: Legal Department.

13.3 Modifications. We may change periodically the Service Offering, the terms of your access to the Service Offering, this Agreement, the Service Description, the Privacy Addendum, the Third Party Terms, the Service Level Agreement, or the Support Policy. It is your responsibility to regularly check the Service Offering and My VMware portals for updates. We will notify you of any material, detrimental change to this Agreement, the Service Description, the Privacy Addendum, the Service Level Agreement, or the Support Policy. In the case of a material, detrimental change to the Service Level Agreement, we will notify you at least 90 days prior to the effective date of the change. The modified Agreement, Service Description, Privacy Addendum, Service Level Agreement, or Support Policy, as applicable, will become effective as of the date stated in that notification. If we make a material, detrimental change to the Service Offering (other than the termination or modification of any beta feature or functionality), this Agreement, the Service Description, the Privacy Addendum, the Service Level Agreement, or the Support Policy, then you may terminate this Agreement no later than 30 days after the effective date of the change. If you terminate this Agreement pursuant to this Section 13.3, the termination will be effective as of the date we receive your notification, unless you state in your notification an effective date that is later but within 45 days after we receive your notification. If you terminate a Subscription-based Service Offering, we will refund any prepaid fees, pro-rated for the remainder of the term, and less any discounts that would not be earned as of the effective date of the termination. Your continued use of the Service Offering after the effective date of any modification to the Agreement, the Service Description, the Privacy Addendum, the Third Party Terms, the Service Level Agreement, or the Support Policy will be deemed acceptance of the modified terms, as applicable.

13.4 Waiver. The waiver of a breach of any provision of this Agreement will not constitute a waiver of any other provision or any later breach.

13.5 Severability. If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions of this Agreement will remain in force.

13.6 Compliance with Laws; Export Control. Each party will comply with all laws applicable to the actions contemplated by this Agreement. You acknowledge that the Service Offering is of United States origin, is provided subject to the U.S. Export Administration Regulations (including "deemed export" and "deemed re-export" regulations), and may be subject to the export control laws of the applicable country. You represent and warrant that (a) you are not, and are not acting on behalf of, (1) any person who is a citizen, national, or resident of, or who is controlled by, the government of any country to which the United States has prohibited export transactions; (2) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List, or any similar designated persons list published for the jurisdiction in which the data center you choose for the Service Offering is located; (b) you will not permit the Service Offering to be used for any purposes prohibited by law, including any prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons; (c) Your Content will not be classified or listed on the United States Munitions list or similar list published for the jurisdiction in which the data center you choose for the Service Offering is located, or contain defense articles, defense services or ITAR-related data; (d) Your Content will not require an export license and is not restricted under applicable export control laws from export to any country where VMware or VMware's service providers maintain facilities or personnel; and (e) you are not subject, either directly or indirectly, to any order issued by any agency of the United States government, revoking or denying, in whole or in part, your United States export privileges. You will notify VMware immediately if you become subject to any such order.

13.7 Government Regulations. For purposes of sales to government entities in the U.S.: The Service Offering and its documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFARS Section 227.7202 and FAR Paragraph 12.212(b), as applicable. Any use, modification, reproduction, release, performing, displaying or disclosing of the Service Offering and documentation by or on behalf of the U.S. Government will be governed solely by the terms and conditions of this Agreement.

13.8 Force Majeure. We will not be liable for any delay or failure to perform any obligations under this Agreement due to any cause beyond our reasonable control, including acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications or other utility failures, earthquakes, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism or war.

13.9 Construction. The headings of sections of this Agreement are for convenience and are not for use in interpreting this Agreement. As used in this Agreement, the word 'including' means "including but not limited to."

13.10 Governing Law. This Agreement is governed by the laws of the State of California, United States of America (excluding its conflict of law rules), except as follows: for Service Offering purchases where you choose a data center that is outside the United States of America, the governing laws are those of the country in which the data center is located (excluding its conflict of law rules). The United Nations Convention for the International Sale of Goods does not apply. This Agreement does not affect your statutory rights that cannot be waived or changed by contract.

13.11 Third Party Rights. Other than as expressly provided in this Agreement, this Agreement does not create any rights for any person who is not a party to it, and no person who is not a party to this Agreement may enforce any of its terms or rely on any exclusion or limitation contained in it.

13.12 Order of Precedence. The terms of this Agreement will supersede and control over any conflicting or additional terms and conditions of any other purchasing related document issued by you.

13.13 Entire Agreement. This Agreement, as it may be revised by us, is the entire agreement of the parties regarding its subject matter. This Agreement supersedes all prior or contemporaneous communications, understandings and agreements, whether written or oral, between the parties regarding its subject matter.

14. Definitions.

Search

14.1 "**Confidential Information**" means non-public technical, business or other information or materials disclosed or otherwise made available by one party in connection with the Service Offering that are in tangible form and clearly labeled "confidential" or the like, or are provided under circumstances reasonably indicating their confidentiality. Our Confidential Information includes: (1) Login Credentials; and (2) any information or materials relating to the Service Offering. (/)

14.2 "**Infringement Claim**" means any third party claim that any VMware Software used to provide the Service Offering infringes any patent, trademark or copyright of the third party, or misappropriates a trade secret (but only to the extent that the misappropriation is not a result of your actions) under the laws of: (a) the United States; (b) Canada; (c) the European Economic Area member states; (d) Australia; (e) New Zealand; (f) Japan; or (g) the People's Republic of China, to the extent that those countries are part of your places of use of the Service Offering.

14.3 "**Intellectual Property Rights**" means all worldwide intellectual property rights, including copyrights, trademarks, service marks, trade secrets, patents, patent applications, and moral rights, whether registered or unregistered.

14.4 "Login Credentials" mean any passwords, authentication keys or security credentials that enable your access to and management of the Service Offering.

14.5 "**OnDemand-based Service Offering**" means a Service Offering for which you pay for actual usage in arrears on a periodic basis, as specified in your Order.

14.6 "**Order**" means the internet order page, or other ordering document, that specifies your purchase of the Service Offering.

14.7 "**Privacy Addendum**" means the then-current version of the Service Offering Data Privacy Addendum document available at http://www.vmware.com/download/eula/horizon-air-data-privacy-addendum.html (http://www.vmware.com/download/eula/horizon-air-data-privacy-addendum.html).

14.8 "**Service Description**" means the then-current version of the Service Offering Service Description document available at http://www.vmware.com/files/pdf/support/horizon-air-service-description.pdf (http://www.vmware.com/files/pdf/support/horizon-air-service-description.pdf) for the Horizon Air Service Offering and http://www.vmware.com/files/pdf/support/horizon-air-hybrid-mode-service-description.pdf (http://www.vmware.com/files/pdf/support/horizon-air-service-description.pdf) for the Horizon Air Hybrid Mode Service Offering, which contains technical and other information.

14.9 "**Service Level Agreement**" means the then-current version of the Service Offering Service Level Agreement document available at www.vmware.com/download/eula/horizon-air-service-license-agreement.html (http://www.vmware.com/download/eula/horizon-air-service-license-agreement.html) for the Horizon Air Service Offering and http://www.vmware.com/download/eula/horizon-air-hybrid-mode-service-level-agreement.html (http://www.vmware.com/download/eula/horizon-air-service-license-agreement.html) for the Horizon Air Hybrid Mode Service Offering.

14.10 "**Subscription-based Service Offering**" means a Service Offering for which you pay in advance for use of the Service Offering for a fixed period as specified in your Order. A Subscription-based Service Offering may also include optional services (e.g., add-ons) and metered usage components.

14.11 "**Support Policy**" means the then-current version of the Service Offering Support Policy document available at https://www.vmware.com/support/policies/saas-support.html (https://www.vmware.com/support/policies/saas-support.html), which we may modify from time to time.

14.12 "**Third Party Content**" means third party data, service, content, software or applications, including open source software.

14.13 "**Third Party Terms**" means the then-current version of the third party terms applicable to Third Party Content that you obtain in connection with the Service Offering that are available at www.vmware.com/files/pdf/support/horizon-air-third-party-terms.pdf (http://www.vmware.com/files/pdf/support/horizon-air-third-party-terms.pdf).

14.14 "**User**" means any person that accesses Your Content or uses the Service Offering under your Login Credentials.

14.15 "**VMware Software**" means the software programs listed in our commercial price list.

14.16 "**Your Content**" means any and all applications, services, files, information, data or other content uploaded to or published or displayed through the Service Offering by you, Users, or us (acting upon your instructions as part of a service).

15. Provisions for Specific Data Centers. For Service Offering purchases where you choose a data center located in the countries listed below, the following provisions replace or supplement the referenced sections of this Agreement, as noted.

15.1 Australian Data Center:

15.1.1 Supplement Section 9 titled "Disclaimer" with the following additional paragraph:
"Nothing in this Agreement (including this Section 9 and Section 1.5) excludes, restricts or modifies any consumer guarantee, right or remedy conferred on you by the Australian Consumer Law or any other applicable law that cannot be excluded, restricted or modified by agreement. Subject to the preceding sentence, any condition, warranty, guarantee, right or liability which would otherwise be implied in this Agreement or imposed by law is excluded. VMware's liability for any breach of any consumer guarantee, right or remedy conferred by the Australian Consumer Law which cannot be excluded is limited, at VMware's option, to supplying the applicable service again or to the payment of the cost of having that service provided again."

Search

15.1.2 Replace the first sentence of Section 13.10 titled "Governing Law" with the following:

"This Agreement is governed by the laws of New South Wales, Australia, without regard to conflict of law principles."

15.2 German Data Center:

(/)

15.2.1 Replace the last sentence of Section 1.4 titled "Third Party Content" with the following sentence:
"Except as permitted under Sections 6 and 7, we will only suspend or terminate Third Party Content during a subscription term with thirty (30) days prior notice, in which case we will provide a pro-rata refund of any pre-payments (if any) made for such suspended or terminated Third Party Content."

15.2.2 In Section 1.5 titled "Evaluation and Beta Use", remove the period at the end of the third sentence which reads "[...] (b) "AS IS", excluding any Service Level Agreement, and without indemnification or warranty or condition of any kind." And add the following to the end of the third sentence:
", except insofar as defects have been fraudulently concealed by us."

15.2.3 Replace Section 7.3 titled "Termination for Insolvency" with the following:
"7.3 [Reserved]"

15.2.4 Replace Section 9 titled "Disclaimer" with the following:

"9. Limited Warranty.

9.1 Qualities. During the Service Offering term, the Service Offering will substantially conform to the applicable Service Description unless otherwise stated herein. We do not commit that the Service Offering will be uninterrupted or that the Service Offering does fulfill any merchantability or fitness for a particular purpose, or will meet (or is designed to meet) your business requirements, unless stated otherwise in the applicable Service Description or individually agreed between the parties.

9.2 Warranty. We will correct any defect in the aforementioned qualities of the Service Offering reported to us by you in writing. If we are unable to correct the defect, we will refund an appropriate portion of the fees paid by you with respect to the affected portion of the affected Service Offering.

9.3 Any Service Credits (as set forth in the Service Level Agreement), will be set off against any refund for breach of warranty, if and to the extent such Service Credits are provided for the same event that entitles you to a refund for breach of warranty.

9.4 Subject to Section 11, the remedies in Section 9.2 are your sole and exclusive remedies for breach of warranty and our sole and exclusive liability for breach of warranty."

15.2.5 Replace Section 11 titled "Limitation of Liability" with the following:

"11.1 Limitation. Our liability for a claim of any nature arising out of this Agreement, regardless of whether the claim is based in contract, tort, strict liability, or otherwise,

11.1.1 will be limited to damages that are foreseeable and typical for this type of contract ("vertragstypische und vorhersehbare Schäden") arising from a slight negligent breach of a material contractual obligation ("Kardinalpflicht", i.e. an obligation the fulfillment of which is essential to enable the proper performance of the contract, and on which fulfillment you may rely on); and

11.1.2 will not exceed per damage event (i) EUR 250.000 (Two Hundred Fifty Thousand Euro), or (ii) if the aggregate fees paid or payable to us for your access to and use of the Service Offering in the twelve (12) months prior to the event giving rise to your claim are higher, then those fees for the specific Service Offering given rise to such claim (subject to the limit set forth in Section 11.1.3 below).

11.1.3 In no event will our total and cumulative liability for all claims arising out of this Agreement exceed EUR 500.000 (Five Hundred Thousand Euro).

11.2 Disclaimer of Liability. In case of slight negligence, we will not be liable for any indirect or consequential damages (including, but not limited to any loss of profits, business opportunity, revenue or goodwill), even if we have been advised as to the possibility of such damages.

11.3 Further Limitations. Our licensors and service providers will have no liability of any kind under this Agreement. You may not bring a claim under this Agreement more than eighteen (18) months after the cause of action arises.

11.4 Exceptions. Nothing in this Agreement will limit or exclude our liability for death or personal injury, for intentional act or gross negligence, fraudulent misrepresentation, fraudulent concealment of a defect, mandatory liability under the German Product Liability Act (Produkthaftungsgesetz), or liability for any damages resulting from a breach of a given guarantee."

15.3 United Kingdom Data Center:

15.3.1 Replace the last sentence in Section 1.4 titled "Third Party Content" with the following sentence:
"Except as permitted under Sections 6 and 7, we will only suspend or terminate Third Party Content during a subscription term with thirty (30) days prior notice, in which case we will provide a pro-rata refund of any pre-payments (if any) made for such suspended orterminated Third Party Content."

Search **15.3.2 Supplement Section 7.3 titled "Termination for Insolvency" with the following:**

(/)

Socialcast Terms of Service

Contact Sales (/company/c...

IMPORTANT-READ CAREFULLY: BY ACCESSING OR USING THE SERVICE, YOU (THE INDIVIDUAL OR LEGAL ENTITY ACCESSING THE HOSTED SERVICE) AGREE TO BE BOUND BY THESE TERMS OF SERVICE ("AGREEMENT"). IF YOU DO NOT AGREE TO THIS AGREEMENT, YOU MUST NOT USE OR ACCESS THE SERVICE, AND YOU MUST NOTIFY THE VENDOR FROM WHICH YOU ACQUIRED ACCESS TO THE SERVICE WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE SUBSCRIPTION FEE, IF ANY, THAT YOU PAID FOR THE SERVICE.

EVALUATION ACCESS. If You are accessing or using the Hosted Service for evaluation purposes, Your use of the Hosted Service is only permitted for evaluation purposes and for the period limited by the Login Credentials. Notwithstanding any other provision in this Agreement, an evaluation of the Hosted Service is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party, an entity that is directly or indirectly controlled by or is under common control with such party, where "control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the relevant entity (but only as long as such person or entity meets these requirements).

1.2 "Customer Data" means any and all files, information, data or other content that You upload to the Hosted Service in connection with Your use of the Hosted Service. It does not include information that VMware collects for relationship management purposes, such as contact, billing, customer relationship management, service delivery, performance measuring, and compliance monitoring.

1.3 "Documentation" means that documentation that is generally provided to You by VMware for the Hosted Service, as revised by VMware from time to time, and which may include service descriptions and access instructions regarding the Hosted Service.

1.4 "Hosted Service" means the VMware hosted offering listed in VMware's commercial price list to which You acquire rights to access and use under an Order.

1.5 "Hosted Service Subscription" means Your right to access and use the Hosted Service as specified in the Documentation for such Hosted Service Subscription during the applicable Hosted Service Subscription Term.

1.6 "Hosted Service Subscription Fee" means the fee, if any, for each Hosted Service Subscription as specified in the Order.

1.7 "Hosted Service Subscription Term" means the time period of Your access to the Hosted Service as specified in the Order.

1.8 "Intellectual Property Rights" means all worldwide intellectual property rights, including without limitation, copyrights, trademarks, service marks, trade secrets, know how, inventions, patents, patent applications, moral rights and all other proprietary rights, whether registered or unregistered.

1.9 "Login Credentials" mean any passwords, authentication keys or security credentials that are provided by VMware to You to enable Your access to the Hosted Service.

1.10 "Order" means (a) a purchase order, enterprise license agreement, or other ordering document issued by You to VMware or a VMware authorized reseller that references and incorporates this Agreement and is accepted by VMware as set forth in Section 4 or (b) an online purchase of the Hosted Service placed via an online store authorized by VMware.

1.11 "Taxes" means any sales, use, gross receipts, business and occupation, and other taxes (other than taxes on VMware's income), export and import fees, customs duties and similar charges applicable to the transactions contemplated by this Agreement that are imposed by any government or other authority.

1.12 "Third Party Agent" means a third party delivering information technology services to You pursuant to a written contract with You.

1.13 "VMware" means VMware, Inc., a Delaware corporation, if You are purchasing Hosted Service Subscriptions for use in the United States and VMware International Limited, a company organized and existing under the laws of Ireland, for all other purchases.

2. ACCESS TO THE SERVICE.

2.1 Provision of Hosted Service. VMware will provide the Hosted Service to You for the type of Hosted Service Subscription specified in the Order during each applicable Hosted Service Subscription Term in accordance with the terms of this Agreement. VMware shall continuously improve and evolve its software products and services offerings and collect and analyze usage patterns, user feedback and other information. Subject to any limitation set forth in Section 12, VMware may change, discontinue, or terminate the Hosted Service or change or remove features or functionality of the Hosted Service in its sole discretion at any time. VMware will notify You of any material change to or termination of the Hosted Service and provide You with a refund of the Hosted Service Subscription Fee pro-rated for the remainder of the Hosted Service Subscription Term.

2.2 Access to Hosted Service. You may access and use the Hosted Service solely for Your own benefit and in accordance with the terms and conditions of this Agreement, the Documentation and any usage restrictions designated in the Order. To the extent that You are given Login Credentials, You shall require that all

authorized users keep Login Credentials strictly confidential and not share such information with any unauthorized person. You are responsible for authorizing and controlling access to the Hosted Service, maintaining the confidentiality of Login Credentials, and for any use that occurs under such Login Credentials.

2.3 Third Party Content. In connection with Your use of the Hosted Service, You may be provided with access to third party data, content, software or applications ("Third Party Content") under separate terms and conditions, including separate fees and charges. Any Third Party Content will be provided "as is" without any representations, warranties or indemnity.

2.4 Third Party Use. Under the access granted to You in Section 2.2 above, You may permit Your Third Party Agents to access, use and/or operate the Hosted Service on Your behalf for the sole purpose of delivering services to You, provided that You will be fully responsible for Your Third Party Agents' compliance with terms and conditions of this Agreement and any breach of this Agreement by a Third Party Agent shall be deemed to be a breach by You.

3. RESTRICTIONS; OWNERSHIP.

3.1 General Restrictions. You acknowledge that the Hosted Service and the structure, organization and source code of the Hosted Service constitute valuable trade secrets of VMware. Accordingly, except as otherwise authorized by VMware in writing, You will not and will not permit any third party to: (a) sell, lease, or provide access to, the Hosted Service to any third party, except as permitted in Section 2.4 above; (b) reverse engineer, or otherwise attempt to derive source code from the Hosted Service, in whole or in part; (c) circumvent, enable, modify or provide access, permissions or rights which violate the technical restrictions of the Hosted Service as described in this Agreement; (d) copy or modify the Hosted Service; (e) interfere with or disrupt the integrity or performance of the Hosted Service or third-party data contained therein; or (f) operate the Hosted Service on behalf of or for the benefit of any third party, including the operation of any service that is accessed by a third party, except that, for the purposes of this Section 3.1 (f), Your Affiliates may use the Hosted Service provided that such use is for such Affiliate's or Your benefit, such use doesn't exceed any usage restrictions in the Order, and You agree to be responsible for such Affiliate's use of the Hosted Service .

3.2 Customer Data.

3.2.1 Customer Data Requirements. As between You and VMware, You and Your authorized users shall retain all right, title and interest in and to the Customer Data and all Intellectual Property Rights therein. Nothing in the Agreement will confer on VMware any right of ownership or interest in the Customer Data or the Intellectual Property rights therein; provided, however, that you consent to VMware's use of Customer Data to provide, improve and manage the Hosted Service in accordance with this Agreement and applicable law. You are solely responsible for the Customer Data that Your authorized users upload, publish, display, link to or otherwise make available (hereinafter, "post") on the Hosted Service, and You agree that VMware is only acting as a passive conduit for the online distribution and publication of the Customer Data. VMware will not review, share, distribute, or reference any such Customer Data except as provided herein or as required by law. You agree to take steps to ensure that Your authorized users do not post Customer Data that: (i) may create a risk of harm, loss, physical or mental injury, emotional distress, death, disability, disfigurement, or physical or mental illness to an authorized user, or any other person or entity; (ii) may create a risk of any other loss or damage to any person or property; (iii) may constitute or contribute to a crime or tort; (iv) contains any information or content that is unlawful, harmful, abusive, racially or ethnically offensive, defamatory, infringing, invasive of personal privacy or publicity rights, harassing, humiliating to other people (publicly or otherwise), libelous, threatening, or otherwise objectionable; (v) contains any information or content that is illegal; or (vi) contains any information or content that You do not have a right to make available under any law or under contractual or fiduciary relationships. You represent and warrant that the Customer Data does not and will not violate third-party rights of any kind, including without limitation any Intellectual Property Rights, rights of publicity and privacy. You shall ensure that your use of the Hosted Service and all Customer Data is at all times compliant with your privacy policies and all applicable local, state, federal and international laws and regulations. VMware is not responsible for any public display or misuse of Customer Data, except in the case of gross negligence or intentional misconduct by VMware or its employees.

3.2.2 Protection of Customer Data. VMware shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data. VMware will not (a) modify Customer Data, (b) disclose Customer Data except as compelled by law in accordance with Section 10.3 or as expressly permitted in writing by You, or (c) access Customer Data except to provide the Hosted Services and prevent or address service or technical problems, or at Your request in connection with customer support matters.

3.2.3 Customer Content Storage. The Service is not an archiving service. Except as expressly set forth in this Agreement, VMware reserves the right to remove Customer Data from the Service at any time and VMware expressly disclaims any obligations with respect to the storage or transfer of Customer Data.

3.2.4 Indemnification by Customer. You shall defend and indemnify VMware against any third party claim arising from or relating to: (a) Customer Data; (b) any infringement or misappropriation of any Intellectual Property Rights by You, Your customers or Your suppliers; (c) violation of law by You; or (d) Your use of the Hosted Service in violation of this Agreement, provided that VMware: (i) provides You with notice of such claim within a reasonable period of time after learning of the claim; and (ii) reasonably cooperates in response to Your requests for assistance. You may not settle or compromise any indemnified claim without the prior written consent of VMware.

3.3 Ownership. The Hosted Service and Documentation, all copies and portions thereof, and all improvements, enhancements, modifications and derivative works thereof, and all Intellectual Property Rights therein, are and shall remain the sole and exclusive property of VMware and its licensors. Your rights to use the Hosted Service and Documentation shall be limited to those expressly granted in this Agreement and any applicable Order. No other rights with respect to the Hosted Service or any related Intellectual Property Rights are implied. The Customer Data, all copies and portions thereof, and all Intellectual Property Rights therein, are and shall remain Your and Your licensors' sole and exclusive property.

4. ORDER.

4.1 Orders. All Orders are subject to this Agreement. No Orders are binding on VMware until accepted by VMware. Orders for the Hosted Service (including any renewal of the Hosted Service) are deemed to be accepted upon VMware's issuance of an invoice for such Hosted Service. Orders issued to VMware do not have to be signed to be valid and enforceable. Notwithstanding the foregoing, if determined by VMware in its sole discretion, Orders for the Hosted Service may be placed via an online store authorized by VMware.

4.2 Purchases through Resellers. The terms of this Agreement related to delivery, pricing, payment or taxes shall not apply to any of Your purchases of the Hosted Service (including any renewal of the Hosted Service) through VMware authorized resellers, and You shall establish such terms independently with the authorized reseller.

4.3 Delivery of Login Credentials. If VMware desires to accept an Order for the Hosted Service, VMware shall deliver the corresponding Hosted Service to You

by emailing the corresponding Login Credentials to You. The Hosted Service shall be deemed delivered and accepted upon VMware emailing the corresponding Login Credentials to You. Notwithstanding the foregoing, the Hosted Service will be delivered via the method specified in the online store, if purchased in an Order via an online store authorized by VMware.

(/)

4.4 Invoicing and Payment Terms. VMware will, upon making the Hosted Service available to You, invoice You for the fees set out in the applicable Order. You shall pay all fees, in the currency specified in the invoice, within thirty (30) days after the date of the invoice. If Your usage of the Hosted Service exceeds the amount for which You have paid, You will promptly pay to VMware any additional fees for all such additional usage by You. Except as expressly set forth in this Agreement, fees are non-refundable and amounts not paid when due shall incur a late fee equal to the lesser of one and one-half percent (1.5%) per month or the maximum amount allowed by applicable law. VMware may suspend the delivery of the Hosted Service while any payment is delinquent. Notwithstanding the foregoing, if You purchase the Hosted Service via an online store authorized by VMware, Your payment terms will be as specified at the time of purchase.

4.5 Taxes. Hosted Service Subscription Fees are exclusive of Taxes and You shall pay or reimburse VMware for all Taxes arising out of this Agreement or the transactions contemplated by this Agreement. If You are required to pay or withhold any Tax in respect of any payments due to VMware hereunder, You shall gross up payments actually made such that VMware shall receive sums due hereunder in full and free of any deduction for any such Tax. You hereby confirm that VMware can rely on the "ship to" name and address set forth in Order You place directly with VMware as being the place of supply for sales tax and income tax purposes. Where VMware is making a supply of services under Article 44 of VAT Directive 2006/112/EC, You confirm that VMware can rely on the "bill to" name and address as per the Order issued by You to VMware as being the place of supply for VAT purposes where You have established its business.

5. SUPPORT AND SUBSCRIPTION SERVICES. Subject to the terms of this Agreement, VMware shall provide support for the Hosted Service to You during the Hosted Service Subscription Term in accordance with the terms specified at www.vmware.com/support/policies/saas-support (/support/policies/saas-support.html).

6. DISCLAIMER. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VMWARE AND ITS LICENSORS DISCLAIM ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE) REGARDING OR RELATING TO THE HOSTED SERVICE, THE DOCUMENTATION, OR ANY MATERIALS OR SERVICES FURNISHED OR PROVIDED TO YOU UNDER THIS AGREEMENT. VMWARE AND ITS LICENSORS DO NOT WARRANT THAT THE HOSTED SERVICE WILL OPERATE UNINTERRUPTED OR THAT IT WILL BE FREE FROM DEFECTS OR THAT THE SERVICE WILL MEET (OR IS DESIGNED TO MEET) YOUR BUSINESS REQUIREMENTS.

7. INTELLECTUAL PROPERTY INDEMNIFICATION.

7.1 Defense and Indemnification. Subject to the remainder of this Section 7, VMware shall defend You against any third party claim that the Hosted Service infringes any patent, trademark or copyright of such third party, or misappropriates a trade secret (but only to the extent that such misappropriation is not a result of Your actions) under the laws of: (a) the United States and Canada; (b) the European Economic Area; (c) Australia; (d) New Zealand; (e) Japan; or (f) China, to the extent that such countries are part of Your places of use of the Hosted Service ("Infringement Claim") and indemnify You from the resulting costs and damages finally awarded against You to such third party by a court of competent jurisdiction or agreed to in settlement; provided that You: (i) provide VMware with notice of such Infringement Claim within a reasonable period of time after learning of the claim; (ii) allow VMware sole control over the defense thereof and related settlement negotiation; and (iii) reasonably cooperate in response to VMware requests for assistance. You may not settle or compromise any Infringement Claim without the prior written consent of VMware.

7.2 Remedies. Should the Hosted Service become, or in VMware's opinion be likely to become, the subject of an Infringement Claim, VMware will, at VMware's option and expense either: (a) procure the rights necessary for You to make continued use of the affected Hosted Service in accordance with this Agreement; (b) modify the affected Hosted Service to make it non-infringing; or (c) terminate Your Hosted Service Subscription to the affected Hosted Service and refund the Hosted Service Subscription Fees paid by You for the affected Hosted Service, pro-rated for the remainder of the Hosted Service Subscription Term.

7.3 Exclusions. Notwithstanding the foregoing, VMware will have no obligation under this Section 7 or otherwise with respect to any claim based on: (a) a combination of the Hosted Service with non-VMware products (other than non-VMware products that are listed on the Order and used in an unmodified form); (b) use of the Hosted Service for a purpose or in a manner not specified in the Documentation; (c) any modification to the Hosted Service made without VMware's express written approval; (d) any claim that relates to Linux or Android open source software, even when it has been embedded into the Hosted Service; or (e) any Hosted Service provided on a no charge, beta or evaluation basis. THIS SECTION 7 STATES YOUR SOLE AND EXCLUSIVE REMEDY AND VMWARE'S ENTIRE LIABILITY FOR ANY INFRINGEMENT CLAIMS OR ACTIONS.

8. LIMITATION OF LIABILITY.

8.1 Limitation of Liability. TO THE MAXIMUM EXTENT MANDATED BY LAW, IN NO EVENT WILL VMWARE AND ITS LICENSORS BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE, LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY, OR OTHERWISE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE PRECEDING LIMITATION MAY NOT APPLY TO YOU. VMWARE'S AND ITS LICENSORS' LIABILITY UNDER THIS AGREEMENT WILL NOT, IN ANY EVENT, REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE, EXCEED THE SUBSCRIPTION FEES YOU PAID FOR THE HOSTED SERVICE IN THE PRIOR TWELVE (12) MONTHS, IF ANY. THE FOREGOING LIMITATIONS SHALL APPLY REGARDLESS OF WHETHER VMWARE OR ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

8.2 Further Limitations. VMware's licensors shall have no liability of any kind under this Agreement and VMware's liability with respect to any third party software or third party content provided with the Hosted Service shall be subject to Section 8.1. You may not bring a claim under this Agreement more than eighteen (18) months after the cause of action arises.

9. TERMINATION.

9.1 Term of Agreement. This Agreement will terminate in its entirety upon the termination of the Hosted Service Subscription Term, unless terminated earlier under this Section 9.

9.2 Termination for Breach. VMware may terminate this Agreement in its entirety effective immediately upon written notice to You if: (a) You breach any provision in Section 3; (b) You fail to pay any portion of the fees under an applicable Order within ten (10) days after receiving written notice from VMware that payment is past due; (c) You breach any other provision of this Agreement and don't not cure the breach within thirty (30) days after receiving written notice thereof from

VMware; or (d) You commit a material breach that is not capable of being cured.

9.3 Termination for Insolvency. VMware may terminate this Agreement in its entirety effective immediately upon written notice to You if You: (a) terminate or suspend Your business; (b) become insolvent, admit in writing Your inability to pay Your debts as they mature, make an assignment for the benefit of creditors; or become subject to control of a trustee, receiver or similar authority; or (c) become subject to any bankruptcy or insolvency proceeding.

9.4 Effect of Termination. If VMware terminates this Agreement under this Section 9: (a) all rights to the Hosted Service granted to You under this Agreement will immediately cease to exist; and (b) You must promptly discontinue all access or use of the Hosted Service, and return, or if requested by VMware, destroy, any related VMware Confidential Information in Your possession or control and certify in writing to VMware that You have fully complied with these requirements. Sections 1 (Definitions), 3 (Restrictions; Ownership), 6 (Disclaimer), 8 (Limitation of Liability), 9 (Termination), 10 (Confidential Information) and 11 (Miscellaneous) will any survive termination of this Agreement.

10. CONFIDENTIAL INFORMATION.

10.1 Definition. "Confidential Information" means information or materials provided by one party ("Discloser") to the other party ("Recipient") which are in tangible form and labeled "confidential" or the like, or, information which a reasonable person knew or should have known to be confidential. The following information shall be considered Confidential Information whether or not marked or identified as such: (a) Login Credentials; (b) information regarding VMware pricing, product roadmaps or strategic marketing plans; and (c) non-public materials relating to the Hosted Service.

10.2 Protection. Recipient may use Confidential Information of Discloser; (a) to exercise its rights and perform its obligations under this Agreement; or (b) in connection with the parties' ongoing business relationship. Recipient will not use any Confidential Information of Discloser for any purpose not expressly permitted by this Agreement, and will disclose the Confidential Information of Discloser only to the employees or contractors of Recipient who have a need to know such Confidential Information for purposes of this Agreement and who are under a duty of confidentiality no less restrictive than Recipient's duty hereunder. Recipient will protect Confidential Information from unauthorized use, access, or disclosure in the same manner as Recipient protects its own confidential or proprietary information of a similar nature but with no less than reasonable care.

10.3 Exceptions. Recipient's obligations under Section 10.2 with respect to any Confidential Information will terminate if Recipient can show by written records that such information: (a) was already known to Recipient at the time of disclosure by Discloser; (b) was disclosed to Recipient by a third party who had the right to make such disclosure without any confidentiality restrictions; (c) is, or through no fault of Recipient has become, generally available to the public; or (d) was independently developed by Recipient without access to, or use of, Discloser's Information. In addition, Recipient will be allowed to disclose Confidential Information to the extent that such disclosure is required by law or by the order of a court of similar judicial or administrative body, provided that Recipient notifies Discloser of such required disclosure promptly and in writing and cooperates with Discloser, at Discloser's request and expense, in any lawful action to contest or limit the scope of such required disclosure.

11. GENERAL

11.1 Assignment. This Agreement and any Orders, and any of Your rights or obligations thereunder, may not be assigned, subcontracted or transferred by You, in whole or in part, whether voluntary, by operation of contract, law or otherwise, without the prior written consent of VMware. Any attempted assignment or transfer in violation of the foregoing will be null and void. Subject to the foregoing, this Agreement will be binding upon and will inure to the benefit of the parties and their respective successors and assigns.

11.2 Notices. Any notice delivered by VMware to You under this Agreement will be delivered via mail, email or fax.

11.3 Waiver. The waiver of a breach of any provision of this Agreement shall not constitute a waiver of any other provision or any subsequent breach.

11.4 Severability. If any provision of this Agreement is held to be illegal, invalid or unenforceable, the provision will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remaining provisions of this Agreement will remain in full force and effect.

11.5 Compliance with Laws; Export Control; Government Regulations. Each party shall comply with all laws applicable to the actions contemplated by this Agreement. You acknowledge that the Hosted Service is of United States origin, is provided subject to the U.S. Export Administration Regulations, may be subject to the export control laws of the applicable territory, and that diversion contrary to applicable export control laws is prohibited. You represent that (1) You are not, and are not acting on behalf of, (a) any person who is a citizen, national, or resident of, or who is controlled by the government of any country to which the United States has prohibited export transactions; or (b) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List; and (2) You will not permit the Hosted Service to be used for, any purposes prohibited by law, including, any prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons. All VMware products, services (including but not limited to pre-packaged professional services offerings and Hosted Services) and publications are commercial in nature. The software, Hosted Services, publications and software documentation are "Commercial Items," as that term is defined in 48 C.F.R.§2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. §252.227-7014(a)(1) and 48 C.F.R. §252.227-7014(a)(5), and used in 48 C.F.R. §12.211, 48 C.F.R. §12.212 and 48 C.F.R. §227.7202, as applicable. Pursuant to 48 C.F.R. §12.211, 48 C.F.R. §12.212, 48 C.F.R.§252.227-7015, 48 C.F.R. §227.7202 through 227.7202-4, 48 C.F.R. §52.227-19 and other relevant sections of the Code of Federal Regulations, as applicable, VMware's publications, commercial computer software, Hosted Services and commercial computer software documentation are distributed and licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in the license agreements and terms of service that accompany the products and software documentation and the terms and conditions herein.

11.6 Construction. The headings of sections of this Agreement are for convenience and are not to be used in interpreting this Agreement. As used in this Agreement, the word 'including' means "including but not limited to."

11.7 Governing Law. This Agreement is governed by the laws of the State of California, United States of America, unless mandated by other law. The United Nations Convention for the International Sale of Goods shall not apply.

11.8 Third Party Rights. Other than as expressly set out in this Agreement, this Agreement does not create any rights for any person who is not a party to it, and no person who is not a party to this Agreement may enforce any of its terms or rely on any exclusion or limitation contained in it.

11.9 Order of Precedence. In the event of conflict or inconsistency among this Agreement and the Order, the following order of precedence shall apply: (a) this Agreement and (b) the Order. The terms of this Agreement shall supersede and control over any conflicting or additional terms and conditions of any Order acknowledgement or confirmation or other document issued by You, unless the parties execute a written agreement expressly indicating: (i) that such Order

shall modify this Agreement; or (ii) that the terms of such Order shall supersede and control in the event of any inconsistency.

11.10 Entire Agreement. This Agreement, including accepted Orders and any amendments hereto, contains the entire agreement of the parties with respect to the subject matter of this Agreement and supersedes all previous or contemporaneous communications, representations, proposals, commitments, understandings and agreements, whether written or oral, between the parties regarding the subject matter hereof. This Agreement may be amended only in writing signed by authorized representatives of both parties.

11.11 Contact Information. Please direct legal notices or other correspondence to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America. If You have any questions concerning this Agreement, please send an email to info@vmware.com.

12. Hosted Service-Specific Terms And Conditions. In addition to the above sections, the Hosted Service is subject to the following terms and conditions. In the event of any conflict between the Hosted Service-specific terms and conditions and Sections 1-11 of this Agreement, the Hosted Service-specific terms and conditions shall control.

Socialcast SaaS
Socialcast Dedicated Cloud

" **Content**" means the audio and visual information, documents, software, products and services contained in or made available to You in the course of using the Hosted Service.

" **Named User**" means a designated user who can access or use the Hosted Service.

" **Private Group**" means a portion of the Hosted Service that can be accessed only after receipt and acceptance of an invitation from You or a Named User.

" **External Contributor**" means an individual who is not a "Named User" but is authorized by You to access and post information to one or more Private Groups but is otherwise prohibited from accessing or using the Hosted Service.

" **Hosted Service**" means the VMware hosted offering listed in VMware's commercial price list to which You acquire rights to access and use under an Order. The Hosted Service, includes, but is not limited to, Content.

" **Freemium Offering**" means the Hosted Service made available by VMware on a no-charge basis for up to a total of fifty (50) Named Users and External Contributors.

" **Named User**" means a designated user who can access or use the Hosted Service.

Subject to the terms and conditions of this Agreement and payment of all fees specified in the applicable Order(s), VMware grants to You, during the Hosted Service Subscription Term, a right to: (i) access and use the Hosted Service by the total number and type of Named Users set forth in the applicable Order and (ii) permit External Contributors to access and use Private Groups.

If You have a total of fifty (50) or fewer Named Users and External Contributors, VMware grants to You a right to access and use the Freemium Offering by the Named Users and External Contributors until either You or VMware terminate such right by providing written notice of termination to the other.

You, not VMware, are solely responsible for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use of all Customer Data, and VMware shall not be responsible or liable for the deletion, correction, destruction, damage, loss or failure to store any Customer Data. Upon the expiration of the Hosted Service Subscription Term, this Agreement will automatically renew, at VMware's then current fees, for successive terms. The length of each renewal term shall be one (1) year, unless otherwise specified in the associated renewal Order. Each renewal term shall be considered a new Hosted Service Subscription Term. Either VMware or You may terminate this Agreement, without cause, or reduce the number of licenses, effective only upon the expiration of the then current Hosted Subscription Term, by notifying the other in writing at least thirty (30) days prior to the expiration of the then current Hosted Service Subscription Term. In the event this Agreement is terminated (other than by reason of Your breach), VMware will make available to You, within 30 days of termination of the Agreement, a file of any Customer Data stored by VMware, if You so request at the time of such termination. VMware does not have any obligation to retain Customer Data, and may delete Customer Data, more than thirty (30) days after any termination of this Agreement.

VMware reserves the right to withhold, remove and/or discard Customer Data, without notice, upon any breach of this Agreement by You. Upon termination of Your access to the Hosted Service or this Agreement for cause, Your right to access or use Customer Data immediately ceases, and VMware shall have no obligation to maintain or to make available or provide to You any Customer Data. VMware shall have the right, but not the obligation, to monitor Customer Data, including chat rooms and forums, and Your use of the Hosted Service to determine compliance with this Agreement and any operating rules established by VMware, to provide support to You and to satisfy any law, regulation or authorized government request. VMware shall have the right in its sole discretion to edit, refuse to post or remove any material submitted to or posted using the Hosted Service. Without limiting the foregoing, VMware shall have the right to remove any material that VMware in its sole discretion, finds to be in violation of the provisions of this Agreement.

VMware may collect certain data and information as a result of Your access or use of the Hosted Service. VMware may share personal information of Yours and the Named Users with its service providers and suppliers to the extent needed to deliver or provide information on products or services or otherwise support Your business needs relating to the Hosted Service. Third party service providers and suppliers receiving any such personal information are expected to apply the same level of privacy protection as VMware. They are required to keep confidential the personal information received from VMware and may not use it for any purpose other than those set forth above.

VMware may reference You as a customer of VMware, which may include a copy of Your corporate logo, unless You provide prior written notice to VMware prohibiting such reference.

In addition to this Agreement, the Hosted Service shall be subject to the terms and conditions of the Socialcast Service Level Agreement.

NOTWITHSTANDING ANY OTHER PROVISION IN THIS AGREEMENT, THE FREEMIUM OFFERING IS PROVIDED "AS-IS" WITHOUT INDEMNIFICATION, SUPPORT OR WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED.

Copyright © 1998-2016

VMware, Inc. All rights reserved. VMware software products are protected by one or more U.S. Patent Numbers

D617,808, D617,809, D617,810, D617,811, 6,256,637, 6,360,219, 6,397,242, 6,496,847, 6,567,905, 6,681,226, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,883,095, 6,940,980, 6,944,699, 6,961,806, 6,961,941, 6,970,562, 7,017,041, 7,055,032, 7,065,642, 7,069,413, 7,069,435, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149,310, 7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999,

7,278,030, 7,281,102, 7,290,253, 7,343,599, 7,356,679, 7,373,355, 7,386,720, 7,409,487, 7,412,492, 7,412,702, 7,424,710, 7,428,636, 7,433,951, 7,434,002, 7,447,854, 7,447,903, 7,467,067, 7,475,002, 7,478,173, 7,478,180, 7,478,218, 7,478,3[illegible]3, 7,487,314, 7,490,216, 7,500,048, 7,506,122, 7,516,453, 7,529,897, 7,555,747, 7,565,527, 7,571,471, 7,577,722, 7,581,064, 7,590,715, 7,590,982, 7,594,111, 7,596,594, 7,596,697, 7,599,493, 7,603,704, 7,606,868, 7,620,523, 7,620,766, 7,620,955, 7,624,240, 7,630,493, 7,636,831, 7,657,659, 7,657,937, 7,665,088, 7,672,814, 7,680,919, 7,693,996, 7,694,101, 7,702,843, 7,707,185, 7,707,285, 7,707,578, 7,716,446, 7,734,045, 7,734,911, 7,734,912, 7,735,136, 7,743,389, 7,761,917, 7,765,543, 7,774,391, 7,779,091, 7,783,779, 7,783,838, 7,793,279, 7,797,748, 7,801,703, 7,802,000, 7,802,248, 7,805,676, 7,814,495, 7,823,145, 7,831,661, 7,831,739, 7,831,761, 7,831,773, 7,840,790, 7,840,839, 7,840,993, 7,844,954, 7,849,098, 7,853,744, 7,853,960, 7,856,419, 7,856,531, 7,856,637, 7,865,663, 7,869,967, 7,886,127, 7,886,148, 7,886,346, 7,890,754, 7,895,437, 7,908,646, 7,912,951, 7,921,197, 7,925,850, 7,933,981, 7,934,017, 7,934,020, 7,941,470, 7,941,827, 7,945,436, 7,945,761, 7,945,908, 7,945,958, 7,953,833, 7,958,558, 7,962,647, 7,966,615, 7,970,938, 7,971,015, 7,971,047, 7,971,182, 7,975,165, 7,984,254, 7,984,264, 7,984,304, 8,001,083, 8,001,322, 8,006,043, 8,010,667, 8,010,676, 8,010,701, 8,013,859, 8,015,367, 8,015,388, 8,019,861, 8,024,506, 8,024,779, 8,028,071, 8,037,032, 8,037,227, 8,037,280, 8,046,468, 8,056,076, 8,060,342, 8,060,722, 8,060,875, 8,060,877, 8,060,883, 8,069,250, 8,074,045, 8,086,822, 8,095,525, 8,095,929, 8,095,931, 8,099,568, 8,099,607, 8,112,505, 8,117,410, 8,127,014, 8,127,107, 8,127,301, 8,141,075, 8,141,163, 8,145,752, 8,145,763, 8,145,836, 8,146,082, 8,151,263, 8,166,107, 8,166,211, 8,166,253, 8,166,349, 8,166,474, 8,166,475, 8,166,554, 8,170,123, 8,171,033, 8,171,140, 8,171,141, 8,171,142, 8,171,278, 8,171,338, 8,171,345, 8,171,482, 8,171,485, 8,171,488, 8,171,548, 8,176,493, 8,195,774, 8,195,866, 8,201,169, 8,204,986, 8,209,343, 8,209,408, 8,209,680, 8,213,608, 8,214,522, 8,214,576, 8,214,802, 8,214,875, 8,219,063, 8,219,779, 8,219,987, 8,225,071, 8,233,882, 8,234,518, 8,239,608, 8,239,646, 8,239,655, 8,244,853, 8,245,081, 8,245,129, 8,245,227, 8,250,197, 8,250,214, 8,250,519, 8,250,586, 8,250,638, 8,255,484, 8,255,806, 8,260,816, 8,260,904, 8,261,265, 8,266,099, 8,266,275, 8,266,279, 8,266,395, 8,266,404, 8,266,628, 8,271,450, 8,275,563, 8,281,318, 8,281,377, 8,286,174, 8,291,135, 8,291,159, 8,291,180, 8,291,436, 8,295,308, 8,296,472, 8,296,551, 8,296,759, 8,296,767, 8,301,874, 8,302,094, 8,307,187, 8,307,191, 8,307,192, 8,312,175, 8,312,471, 8,312,522, 8,316,193, 8,316,374, 8,321,643, 8,321,842, 8,321,850, 8,327,059, 8,332,921, 8,335,703, 8,336,049, 8,340,287, 8,341,749, 8,347,263, 8,347,344, 8,352,240, 8,352,482, 8,352,490, 8,352,705, 8,352,944, 8,359,374, 8,359,422, 8,359,451, 8,359,593, 8,364,932, 8,380,747, 8,380,939, 8,392,361, 8,392,838, 8,397,038, 8,402,224, 8,402,441, 8,402,527, 8,407,475, 8,407,518, 8,412,910, 8,417,812, 8,429,647, 8,429,665, 8,438,430, 8,441,494, 8,443,139, 8,443,156, 8,443,166, 8,443,261, 8,443,367, 8,448,022, 8,453,108, 8,453,143, 8,458,318, 8,458,329, 8,463,730, 8,463,905, 8,464,022, 8,464,259, 8,468,310, 8,473,946, 8,473,947, 8,478,725, 8,478,801, 8,478,924, 8,479,195, 8,543,781, 8,543,790, 8,544,010, 8,484,405, 8,489,636, 8,489,699, 8,489,719, 8,489,800, 8,490,085, 8,495,631, 8,498,987, 8,499,004, 8,499,297, 8,510,438, 8,510,590, 8,510,827, 8,521,504, 8,521,686, 8,521,666, 8,522,228, 8,527,673, 8,528,107, 8,533,382, 8,553,745, 8,543,781, 8,543,790, 8,544,010, 8,549,241, 8,549,364, 8,554,900, 8,554,981, 8,555,003, 8,555,081, 8,555,274, 8,560,577, 8,560,626, 8,560,747, 8,560,791, 8,561,061, 8,566,502, 8,566,744, 8,572,606, 8,572,608, 8,577,853, 8,577,937, 8,578,083, 8,578,380, 8, 583,875, 8,584,126, 8,589,913, 8,589,940, 8,595,369, 8,595,460, 8,595,487, 8,595,824, 8,607,011, 8,607,013, 8,612,659, 8,615,489, 8,619,771, 8,621,136, 8,621,607, 8,626,723, 8,631,065, 8,631,066, 8,631,117, 8,631,403, 8,635,330, 8,635,395, 8635,493, 8,639,917, 8,640,126, 8,650,359, 8,650,566, 8,650,564, 8,656,000, 8,655,971, 8,656,222, 8,656,389, 8,656,497, 8,661,182, 8,661,213, 8,661,428, 8,666,938, 8,667,187, 8,667,459, 8,667,500, 8,671,238, 8,677,085, 8,667,187, 8,677,351, 8,667,352, 8,683,041, 8,683,466, 8,688,823, 8,694,713, 8,694,728, 8,694,746 8,694,828, 8,700,585, 8,700,611, 8,701,107, 8,706,991, 8,707,035, 8,712,960, 8,713,273, 8,713,646, 8,717,895, 8,718,070, 8,719,401, 8,719,513, 8,719,545, 8,719,661, 8,719,800, 8,719,817, 8,719,823, 8,724,696, 8,725,886, 8,726,273, 8,726,225, 8,732,313, 8,732,700, 8,738,333, 8,738,868, 8,743,888, 8,743,889, 8,745,236, 8,745,241, 8,745,308, 8,745,336, 8,745,351, 8,750,119, 8,750,164, 8,751,867, 8,752,058, 8,756,397, 8,756,426, 8,763,115, 8,761,036, 8,762,660, 8,762,684, 8,769,174, 8,769,184, 8,775,594, 8,775,696, 8,775,748, 8,775,773, 8,775,774, 8,775,815, 8,775,903, 8,776,055, 8,776,089, 8,782,242, 8,782,310, 8,782,768, 8,788,079, 8,789,049, 8,793,428, 8,798,541, 8,799,418, 8,799,897, 8,799,921, 8,880,018, 8,805,934, 8,806,217, 8,806,484, 8,812,876, 8,813,074, 8,819,357, 8,817,620, 8,817,621, 8,819,674, 8,819,676, 8,819,822, 8,825,851, 8,825,909, 8,826,273, 8,826,278, 8,826,283, 8,826,289, 8,826,432, 8,825,994, 8,830,823, 8,830, 8,358,832,351, 8,832,390, 8,832,682, 8,832,785, 8,837,493, 8,839,201, 8,839,202, 8,839,266, 8,839,914, 8,838,756, 8,842,679, 8,843,933, 8,843,935, 8,850,004, 8,856,784, 8,862,695, 8,862,868, 8,863,127, 8,868,610, 8,868,880, 8,869,139, 8,874,744, 8,874,859, 8,875,162, 8,875,266, 8,875,288, 8,874,802, 8,874,803, 8,880,468, 8,880,470, 8,880,774, 8,880,930, 8,881,143, 8,886,708, 8,886,865, 8,892,737, 8,892,706, 8,892,776, 8,893,261, 8,892,716, 8,892,706, 8,892,716, 8,892,737, 8,892,776, 8,893,261, 8,898,108, 8,898,676, 8,898,508, 8,898,509, 8,898,518, 8,902,248, 8,902,242, 8,904,081, 8,910,297, 8,909,602, 8,909,928, 8,910,161, 8,910,228, 8,913,483, 8,913,611, 8,914,013, 8,914,567, 8,914,575, 8,914,598, 8,914,610, 8,914,684, 8,914,730, 8,917,617, 8,924,524, 8,924,534, 8,924,608, 8,924,967, 8,924,970, 8,925,036, 8,929,287, 8,930,592, 8,930,812, 8,930,948, 8,935,429, 8,935,456, 8,935,500, 8,938,680, 8,943,259, 8,943,296, 8,949,295, 8,949,399, 8,949,531, 8,949,546, 8,949,570, 8,949,585, 8,949,731, 8,949,791, 8,849,794, 8,949,817, 8,954,050, 8,954,387, 8,954,545, 8,954,575, 8,954,665, 8,955,072, 8,955,151, 8,958,292, 8,958,298, 8,959,215, 8,959,312, 8,959,338, 8,959,529, 8,964,528, 8,964,598, 8,964,767, 8,966,024, 8,966,029, 8,966,035, 8,966,040, 8,966,479, 8,966,581, 8,966,623, 8,972,981, 8,977,702, 8,977,736, 8,978,053, 8,978,110, 8,983,988, 8,984,508, 8,990,531, 8,990,699, 8,995,763, 8,996,853, 8,996,884, 8,997,187, 9,003,027, 9,003,037, 9,007,903, 9,008,087, 9,009,219, 9,009,727, 9,007,903, 9,008,087, 9,009,727, 9,015,180, 9,015,203, 9,015,823, 9,019,826, 9,019,977, 9,021,037, 9,026,510, 9,026,613, 9,026,630, 9,027,003, 9,027,031, 9,031,894, 9,032,050, 9,032,133, 9,032,170, 9,032,176, 9,032,181, 9,032,398, 9,032,402, 9,032,425, 9,037,522, 9,037,556, 9,037,621, 9,037,689, 9,037,719, 9,037,758, 9,037,873, 9,038,066, 9,042,304, 9,043,452, 9,043,792, 9,047,083, 9,047,087, 9,047,133, 9,049,153, 9,049,193, 9,049,257, 9,052,825, 9,052,937, 9,052,949, 9,052,961, 9,052,967, 9,053,064, 9,053,065, 9,054,995, 9,055,119, 9,058,232, 9,058,259, 9,058,353, 9,058,420, 9,058,495, 9,059,964, 9,059,989, 9,059,999, 9,063,756, 9,063,762, 9,063,766, 9,063,768, 9,063,866, 9,064,447, 9,069,579, 9,069,600, 9,069,607, 9,069,608, 9,069,902 , 9,075,718, 9,075,731, 9,077,664, 9,077,725, 9,081,536, 9,081,622, 9,081,686, 9,081,722, 9,083,606, 9,086,904, 9,086,921, 9,086,981, 9,087,191, 9,088,591, 9,092,318, 9,094,413, 9,097,528, 9,098,318, 9,098,347, 9,098,457, 9,099,974, 9,100,293, 9,104,402, 9,104, 469, 9,106,587, 9,116,726, 9,116,829, 9,116,737, 9,116,903, 9,122,594, 9,122,765, 9,123,031, 9,124,488, 9,124,538, 9,128,746, 9,129,062, 9,130,821, 9,130,879, 9,134,922, 9,134,992, 9,135,050, 9,135,171, 9,135,287, 9,135,342, 9,135,457, 9,137,052, 9,137,107, 9,137,222, 9,141,444, 9,141,578, 9,142,004, 9,141,381, 9,146,712, 9,146,721, 9,146,758, 9,146,766, 9,146,841, 9,146,847, 9,148,416, 9,152,445, 9,152,448, 9,152,548, 9,152,570, 9,152,572, 9,154,433, 9,158,434, 9,158,550, 9,158,561, 9,158,601, 9,158,665, 9,160,612, 9,160,630, 9,164,695, 9,166,895, 9,167,104, 9,170,798, 9,170,924, 9,171,139, 9,172,603, 9,172,663, 9,176,780, 9,177,250, 9,178,833, 9,182,927, 9,183,015, 9,183,016, 9,183,034, 9,183,093, 9,183,099, 9,183,101, 9,183,103, 9,183,151, 9,185,069, 9,185,099, 9,189,265, 9,189,410, 9,189,419, 9,189,513, 9,189,609, 9,189,622, 9,189,758, 9,191,384, 9,195,393, 9,195,487, 9,195,491, 9,195,518, 9,195,585, 9,195,707, 9,195,811, 9,197,529, 9,201,646, 9,201,653, 9,201,667, 9,201,674, 9,201,755, 9,202,025, 9,203,701, 9,203,703, 9,203,820, 9,208,015, 9,209,998, 9,210,079, 9,213,544, 9,213,556, 9,213,565, 9,213,570, 9,213,572, 9,213,651, 9,213,851,9,213,852, 9,213,859, 9,214,004, 9,215,177, 9,215,210, 9,215,213, 9,215,214, 9,218,140, 9,218,200, 9,219,813, 9,219,741, 9,223,608, 9,223,722, 9,223,767, 9,225,597, 9,225,638, 9,225,647, 9,225,742, 9,226,155, 9,229,754, 9,230,001, 9,231,818, 9,231,882, 9,231,891, 9,231,892, 9,235,577, 9,237,147, 9,239,682, 9,239,729, 9,239,731, 9,239,776, 9,239,841, 9,244,669, 9,244,717, 9,244,732, 9,244,742, 9,244,755, 9,244,903, 9,245,000, 9,246,833, 9,246,877, 9,246,918, 9,247,042, 9,247,432, 9,250,827, 9,250,854, 9,250,943, 9,251,102, 9,251,103, 9,235,109, 9,253,158, 9,253,309, 9,256,353, 9,256,515, 9,256,746, 9,257,092, 9,258,301, 9,258,359, 9,262,189, 9,262,192, 9,262,198, 9,262,214, 9,264,517, 9,262,750, 9,264,313, 9,264,330, 9,264,704, 9,268,549, 9,268,590, 9,268,591, 9,268,592, 9,268,610, 9,268,642, 9,268,836, 9,270,777, 9,274,814, 9,274,821, 9,274,834, 9,274,974, 9,275,245, 9,276,809, 9,276,897, 9,276,904, 9,277,237, 9,280,300, 9,280,358, 9,280,665, 9,282,019, D751,082, 9,285,993, 9,285,999, 9,286,095, 9,286,102, 9,288,081, 9,288,104, 9,288,259, 9,292,281, 9,292,353, 9,292,401, 9,292,416, 9,292,422, 9,292,452, 9,292,507, 9,292,699, 9,293,376, 9,294,407, 9,294,524, 9,298,375, 9,298,377, 9,298,490, 9,298,512, 9,298,538, 9,298,936, 9,300,593, 9,300,603, 9,304,662, 9,304,705, 9,304,803, 9,304,804, 9,304,873, 9,304,878, 9,304,915, 9,305,014, 9,306,843, 9,306,864, 9,306,909, 9,306,910, 9,306,875, 9,311,129, 9,311,140, 9,311,313, 9,311,464, 9,311,475, 9,313,129, 9,313,263, 9,317,207, 9,317,260, 9,317,315, 9,317,318, 9,317,326, 9,317,333, 9,317,387, 9,317,444, 9,319,288, 9,319,336, 9,319,337, 9,319,338, 9,319,375, 9,323,550, 9,323,565, 9,323,579, 9,325,713, D754,692, 9,329,855, 9,329,889, 9,329,894, 9,329,896, 9,329,958, 9,330,015, 9,330,424, 9,331,937, 9,331,938;patents pending.

Search

CONTACT SALES (/COMPANY/CONTACT_SALES.HTML) GET SUPPORT (/SUPPORT.HTML)
ABOUT VMWARE (/COMPANY.HTML) CAREERS (HTTPS://CAREERS.VMWARE.COM)

© 2017 VMware, Inc

Terms of Use (/help/legal.html)
Privacy (/help/privacy.html)
Accessibility (/help/accessibility.html)
Site Index (/site_index.html)
Trademarks (/help/trademarks.html)
Help (/help.html)
Feedback

(https://twitter.com/VMware) (https://www.facebook.com/vmware) (https://www.linkedin.com/company/vmware)
(http://www.youtube.com/user/vmwaretv) (https://plus.google.com/+vmware)

(/)

(/)

(/)

(/)

Socialcast Terms of Service

Contact Sales (/company/c...

IMPORTANT-READ CAREFULLY: BY ACCESSING OR USING THE SERVICE, YOU (THE INDIVIDUAL OR LEGAL ENTITY ACCESSING THE HOSTED SERVICE) AGREE TO BE BOUND BY THESE TERMS OF SERVICE ("AGREEMENT"). IF YOU DO NOT AGREE TO THIS AGREEMENT, YOU MUST NOT USE OR ACCESS THE SERVICE, AND YOU MUST NOTIFY THE VENDOR FROM WHICH YOU ACQUIRED ACCESS TO THE SERVICE WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE SUBSCRIPTION FEE, IF ANY, THAT YOU PAID FOR THE SERVICE.

EVALUATION ACCESS. If You are accessing or using the Hosted Service for evaluation purposes, Your use of the Hosted Service is only permitted for evaluation purposes and for the period limited by the Login Credentials. Notwithstanding any other provision in this Agreement, an evaluation of the Hosted Service is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party, an entity that is directly or indirectly controlled by or is under common control with such party, where "control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the relevant entity (but only as long as such person or entity meets these requirements).

1.2 "Customer Data" means any and all files, information, data or other content that You upload to the Hosted Service in connection with Your use of the Hosted Service. It does not include information that VMware collects for relationship management purposes, such as contact, billing, customer relationship management, service delivery, performance measuring, and compliance monitoring.

1.3 "Documentation" means that documentation that is generally provided to You by VMware for the Hosted Service, as revised by VMware from time to time, and which may include service descriptions and access instructions regarding the Hosted Service.

1.4 "Hosted Service" means the VMware hosted offering listed in VMware's commercial price list to which You acquire rights to access and use under an Order.

1.5 "Hosted Service Subscription" means Your right to access and use the Hosted Service as specified in the Documentation for such Hosted Service Subscription during the applicable Hosted Service Subscription Term.

1.6 "Hosted Service Subscription Fee" means the fee, if any, for each Hosted Service Subscription as specified in the Order.

1.7 "Hosted Service Subscription Term" means the time period of Your access to the Hosted Service as specified in the Order.

1.8 "Intellectual Property Rights" means all worldwide intellectual property rights, including without limitation, copyrights, trademarks, service marks, trade secrets, know how, inventions, patents, patent applications, moral rights and all other proprietary rights, whether registered or unregistered.

1.9 "Login Credentials" mean any passwords, authentication keys or security credentials that are provided by VMware to You to enable Your access to the Hosted Service.

1.10 "Order" means (a) a purchase order, enterprise license agreement, or other ordering document issued by You to VMware or a VMware authorized reseller that references and incorporates this Agreement and is accepted by VMware as set forth in Section 4 or (b) an online purchase of the Hosted Service placed via an online store authorized by VMware.

1.11 "Taxes" means any sales, use, gross receipts, business and occupation, and other taxes (other than taxes on VMware's income), export and import fees, customs duties and similar charges applicable to the transactions contemplated by this Agreement that are imposed by any government or other authority.

1.12 "Third Party Agent" means a third party delivering information technology services to You pursuant to a written contract with You.

1.13 "VMware" means VMware, Inc., a Delaware corporation, if You are purchasing Hosted Service Subscriptions for use in the United States and VMware International Limited, a company organized and existing under the laws of Ireland, for all other purchases.

2. ACCESS TO THE SERVICE.

2.1 Provision of Hosted Service. VMware will provide the Hosted Service to You for the type of Hosted Service Subscription specified in the Order during each applicable Hosted Service Subscription Term in accordance with the terms of this Agreement. VMware shall continuously improve and evolve its software products and services offerings and collect and analyze usage patterns, user feedback and other information. Subject to any limitation set forth in Section 12, VMware may change, discontinue, or terminate the Hosted Service or change or remove features or functionality of the Hosted Service in its sole discretion at any time. VMware will notify You of any material change to or termination of the Hosted Service and provide You with a refund of the Hosted Service Subscription Fee pro-rated for the remainder of the Hosted Service Subscription Term.

2.2 Access to Hosted Service. You may access and use the Hosted Service solely for Your own benefit and in accordance with the terms and conditions of this Agreement, the Documentation and any usage restrictions designated in the Order. To the extent that You are given Login Credentials, You shall require that all

authorized users keep Login Credentials strictly confidential and not share such information with any unauthorized person. You are responsible for authorizing and controlling access to the Hosted Service, maintaining the confidentiality of Login Credentials, and for any use that occurs under such Login Credentials.

(j)

2.3 Third Party Content. In connection with Your use of the Hosted Service, You may be provided with access to third party data, content, software or applications ("Third Party Content") under separate terms and conditions, including separate fees and charges. Any Third Party Content will be provided "as is" without any representations, warranties or indemnity.

2.4 Third Party Use. Under the access granted to You in Section 2.2 above, You may permit Your Third Party Agents to access, use and/or operate the Hosted Service on Your behalf for the sole purpose of delivering services to You, provided that You will be fully responsible for Your Third Party Agents' compliance with terms and conditions of this Agreement and any breach of this Agreement by a Third Party Agent shall be deemed to be a breach by You.

3. RESTRICTIONS; OWNERSHIP.

3.1 General Restrictions. You acknowledge that the Hosted Service and the structure, organization and source code of the Hosted Service constitute valuable trade secrets of VMware. Accordingly, except as otherwise authorized by VMware in writing, You will not and will not permit any third party to: (a) sell, lease, or provide access to, the Hosted Service to any third party, except as permitted in Section 2.4 above; (b) reverse engineer, or otherwise attempt to derive source code from the Hosted Service, in whole or in part; (c) circumvent, enable, modify or provide access, permissions or rights which violate the technical restrictions of the Hosted Service as described in this Agreement; (d) copy or modify the Hosted Service; (e) interfere with or disrupt the integrity or performance of the Hosted Service or third-party data contained therein; or (f) operate the Hosted Service on behalf of or for the benefit of any third party, including the operation of any service that is accessed by a third party, except that, for the purposes of this Section 3.1 (f), Your Affiliates may use the Hosted Service provided that such use is for such Affiliate's or Your benefit, such use doesn't exceed any usage restrictions in the Order, and You agree to be responsible for such Affiliate's use of the Hosted Service .

3.2 Customer Data.

3.2.1 Customer Data Requirements. As between You and VMware, You and Your authorized users shall retain all right, title and interest in and to the Customer Data and all Intellectual Property Rights therein. Nothing in the Agreement will confer on VMware any right of ownership or interest in the Customer Data or the Intellectual Property rights therein; provided, however, that you consent to VMware's use of Customer Data to provide, improve and manage the Hosted Service in accordance with this Agreement and applicable law. You are solely responsible for the Customer Data that Your authorized users upload, publish, display, link to or otherwise make available (hereinafter, "post") on the Hosted Service, and You agree that VMware is only acting as a passive conduit for the online distribution and publication of the Customer Data. VMware will not review, share, distribute, or reference any such Customer Data except as provided herein or as required by law. You agree to take steps to ensure that Your authorized users do not post Customer Data that: (i) may create a risk of harm, loss, physical or mental injury, emotional distress, death, disability, disfigurement, or physical or mental illness to an authorized user, or any other person or entity; (ii) may create a risk of any other loss or damage to any person or property; (iii) may constitute or contribute to a crime or tort; (iv) contains any information or content that is unlawful, harmful, abusive, racially or ethnically offensive, defamatory, infringing, invasive of personal privacy or publicity rights, harassing, humiliating to other people (publicly or otherwise), libelous, threatening, or otherwise objectionable; (v) contains any information or content that is illegal; or (vi) contains any information or content that You do not have a right to make available under any law or under contractual or fiduciary relationships. You represent and warrant that the Customer Data does not and will not violate third-party rights of any kind, including without limitation any Intellectual Property Rights, rights of publicity and privacy. You shall ensure that your use of the Hosted Service and all Customer Data is at all times compliant with your privacy policies and all applicable local, state, federal and international laws and regulations. VMware is not responsible for any public display or misuse of Customer Data, except in the case of gross negligence or intentional misconduct by VMware or its employees.

3.2.2 Protection of Customer Data. VMware shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data. VMware will not (a) modify Customer Data, (b) disclose Customer Data except as compelled by law in accordance with Section 10.3 or as expressly permitted in writing by You, or (c) access Customer Data except to provide the Hosted Services and prevent or address service or technical problems, or at Your request in connection with customer support matters.

3.2.3 Customer Content Storage. The Service is not an archiving service. Except as expressly set forth in this Agreement, VMware reserves the right to remove Customer Data from the Service at any time and VMware expressly disclaims any obligations with respect to the storage or transfer of Customer Data.

3.2.4 Indemnification by Customer. You shall defend and indemnify VMware against any third party claim arising from or relating to: (a) Customer Data; (b) any infringement or misappropriation of any Intellectual Property Rights by You, Your customers or Your suppliers; (c) violation of law by You; or (d) Your use of the Hosted Service in violation of this Agreement, provided that VMware: (i) provides You with notice of such claim within a reasonable period of time after learning of the claim; and (ii) reasonably cooperates in response to Your requests for assistance. You may not settle or compromise any indemnified claim without the prior written consent of VMware.

3.3 Ownership. The Hosted Service and Documentation, all copies and portions thereof, and all improvements, enhancements, modifications and derivative works thereof, and all Intellectual Property Rights therein, are and shall remain the sole and exclusive property of VMware and its licensors. Your rights to use the Hosted Service and Documentation shall be limited to those expressly granted in this Agreement and any applicable Order. No other rights with respect to the Hosted Service or any related Intellectual Property Rights are implied. The Customer Data, all copies and portions thereof, and all Intellectual Property Rights therein, are and shall remain Your and Your licensors' sole and exclusive property.

4. ORDER.

4.1 Orders. All Orders are subject to this Agreement. No Orders are binding on VMware until accepted by VMware. Orders for the Hosted Service (including any renewal of the Hosted Service) are deemed to be accepted upon VMware's issuance of an invoice for such Hosted Service. Orders issued to VMware do not have to be signed to be valid and enforceable. Notwithstanding the foregoing, if determined by VMware in its sole discretion, Orders for the Hosted Service may be placed via an online store authorized by VMware.

4.2 Purchases through Resellers. The terms of this Agreement related to delivery, pricing, payment or taxes shall not apply to any of Your purchases of the Hosted Service (including any renewal of the Hosted Service) through VMware authorized resellers, and You shall establish such terms independently with the authorized reseller.

4.3 Delivery of Login Credentials. If VMware desires to accept an Order for the Hosted Service, VMware shall deliver the corresponding Hosted Service to You

by emailing the corresponding Login Credentials to You. The Hosted Service shall be deemed delivered and accepted upon VMware emailing the corresponding Login Credentials to You. Notwithstanding the foregoing, the Hosted Service will be delivered via the method specified in the online store, if purchased in an Order via an online store authorized by VMware.

(/)

4.4 Invoicing and Payment Terms. VMware will, upon making the Hosted Service available to You, invoice You for the fees set out in the applicable Order. You shall pay all fees, in the currency specified in the invoice, within thirty (30) days after the date of the invoice. If Your usage of the Hosted Service exceeds the amount for which You have paid, You will promptly pay to VMware any additional fees for all such additional usage by You. Except as expressly set forth in this Agreement, fees are non-refundable and amounts not paid when due shall incur a late fee equal to the lesser of one and one-half percent (1.5%) per month or the maximum amount allowed by applicable law. VMware may suspend the delivery of the Hosted Service while any payment is delinquent. Notwithstanding the foregoing, if You purchase the Hosted Service via an online store authorized by VMware, Your payment terms will be as specified at the time of purchase.

4.5 Taxes. Hosted Service Subscription Fees are exclusive of Taxes and You shall pay or reimburse VMware for all Taxes arising out of this Agreement or the transactions contemplated by this Agreement. If You are required to pay or withhold any Tax in respect of any payments due to VMware hereunder, You shall gross up payments actually made such that VMware shall receive sums due hereunder in full and free of any deduction for any such Tax. You hereby confirm that VMware can rely on the "ship to" name and address set forth in Order You place directly with VMware as being the place of supply for sales tax and income tax purposes. Where VMware is making a supply of services under Article 44 of VAT Directive 2006/112/EC, You confirm that VMware can rely on the "bill to" name and address as per the Order issued by You to VMware as being the place of supply for VAT purposes where You have established its business.

5. SUPPORT AND SUBSCRIPTION SERVICES. Subject to the terms of this Agreement, VMware shall provide support for the Hosted Service to You during the Hosted Service Subscription Term in accordance with the terms specified at www.vmware.com/support/policies/saas-support (/support/policies/saas-support.html).

6. DISCLAIMER. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VMWARE AND ITS LICENSORS DISCLAIM ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE) REGARDING OR RELATING TO THE HOSTED SERVICE, THE DOCUMENTATION, OR ANY MATERIALS OR SERVICES FURNISHED OR PROVIDED TO YOU UNDER THIS AGREEMENT. VMWARE AND ITS LICENSORS DO NOT WARRANT THAT THE HOSTED SERVICE WILL OPERATE UNINTERRUPTED OR THAT IT WILL BE FREE FROM DEFECTS OR THAT THE SERVICE WILL MEET (OR IS DESIGNED TO MEET) YOUR BUSINESS REQUIREMENTS.

7. INTELLECTUAL PROPERTY INDEMNIFICATION.

7.1 Defense and Indemnification. Subject to the remainder of this Section 7, VMware shall defend You against any third party claim that the Hosted Service infringes any patent, trademark or copyright of such third party, or misappropriates a trade secret (but only to the extent that such misappropriation is not a result of Your actions) under the laws of: (a) the United States and Canada; (b) the European Economic Area; (c) Australia; (d) New Zealand; (e) Japan; or (f) China, to the extent that such countries are part of Your places of use of the Hosted Service ("Infringement Claim") and indemnify You from the resulting costs and damages finally awarded against You to such third party by a court of competent jurisdiction or agreed to in settlement; provided that You: (i) provide VMware with notice of such Infringement Claim within a reasonable period of time after learning of the claim; (ii) allow VMware sole control over the defense thereof and related settlement negotiation; and (iii) reasonably cooperate in response to VMware requests for assistance. You may not settle or compromise any Infringement Claim without the prior written consent of VMware.

7.2 Remedies. Should the Hosted Service become, or in VMware's opinion be likely to become, the subject of an Infringement Claim, VMware will, at VMware's option and expense either: (a) procure the rights necessary for You to make continued use of the affected Hosted Service in accordance with this Agreement; (b) modify the affected Hosted Service to make it non-infringing; or (c) terminate Your Hosted Service Subscription to the affected Hosted Service and refund the Hosted Service Subscription Fees paid by You for the affected Hosted Service, pro-rated for the remainder of the Hosted Service Subscription Term.

7.3 Exclusions. Notwithstanding the foregoing, VMware will have no obligation under this Section 7 or otherwise with respect to any claim based on: (a) a combination of the Hosted Service with non-VMware products (other than non-VMware products that are listed on the Order and used in an unmodified form); (b) use of the Hosted Service for a purpose or in a manner not specified in the Documentation; (c) any modification to the Hosted Service made without VMware's express written approval; (d) any claim that relates to Linux or Android open source software, even when it has been embedded into the Hosted Service; or (e) any Hosted Service provided on a no charge, beta or evaluation basis. THIS SECTION 7 STATES YOUR SOLE AND EXCLUSIVE REMEDY AND VMWARE'S ENTIRE LIABILITY FOR ANY INFRINGEMENT CLAIMS OR ACTIONS.

8. LIMITATION OF LIABILITY.

8.1 Limitation of Liability. TO THE MAXIMUM EXTENT MANDATED BY LAW, IN NO EVENT WILL VMWARE AND ITS LICENSORS BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE, LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY, OR OTHERWISE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE PRECEDING LIMITATION MAY NOT APPLY TO YOU. VMWARE'S AND ITS LICENSORS' LIABILITY UNDER THIS AGREEMENT WILL NOT, IN ANY EVENT, REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE, EXCEED THE SUBSCRIPTION FEES YOU PAID FOR THE HOSTED SERVICE IN THE PRIOR TWELVE (12) MONTHS, IF ANY. THE FOREGOING LIMITATIONS SHALL APPLY REGARDLESS OF WHETHER VMWARE OR ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

8.2 Further Limitations. VMware's licensors shall have no liability of any kind under this Agreement and VMware's liability with respect to any third party software or third party content provided with the Hosted Service shall be subject to Section 8.1. You may not bring a claim under this Agreement more than eighteen (18) months after the cause of action arises.

9. TERMINATION.

9.1 Term of Agreement. This Agreement will terminate in its entirety upon the termination of the Hosted Service Subscription Term, unless terminated earlier under this Section 9.

9.2 Termination for Breach. VMware may terminate this Agreement in its entirety effective immediately upon written notice to You if: (a) You breach any provision in Section 3; (b) You fail to pay any portion of the fees under an applicable Order within ten (10) days after receiving written notice from VMware that payment is past due; (c) You breach any other provision of this Agreement and don't not cure the breach within thirty (30) days after receiving written notice thereof from

VMware; or (d) You commit a material breach that is not capable of being cured.

9.3 Termination for Insolvency. VMware may terminate this Agreement in its entirety effective immediately upon written notice to You if You: (a) terminate or suspend Your business; (b) become insolvent, admit in writing Your inability to pay Your debts as they mature, make an assignment for the benefit of creditors; or become subject to control of a trustee, receiver or similar authority; or (c) become subject to any bankruptcy or insolvency proceeding.

9.4 Effect of Termination. If VMware terminates this Agreement under this Section 9: (a) all rights to the Hosted Service granted to You under this Agreement will immediately cease to exist; and (b) You must promptly discontinue all access or use of the Hosted Service, and return, or if requested by VMware, destroy, any related VMware Confidential Information in Your possession or control and certify in writing to VMware that You have fully complied with these requirements. Sections 1 (Definitions), 3 (Restrictions; Ownership), 6 (Disclaimer), 8 (Limitation of Liability), 9 (Termination), 10 (Confidential Information) and 11 (Miscellaneous) will any survive termination of this Agreement.

10. CONFIDENTIAL INFORMATION.

10.1 Definition. "Confidential Information" means information or materials provided by one party ("Discloser") to the other party ("Recipient") which are in tangible form and labeled "confidential" or the like, or, information which a reasonable person knew or should have known to be confidential. The following information shall be considered Confidential Information whether or not marked or identified as such: (a) Login Credentials; (b) information regarding VMware pricing, product roadmaps or strategic marketing plans; and (c) non-public materials relating to the Hosted Service.

10.2 Protection. Recipient may use Confidential Information of Discloser; (a) to exercise its rights and perform its obligations under this Agreement; or (b) in connection with the parties' ongoing business relationship. Recipient will not use any Confidential Information of Discloser for any purpose not expressly permitted by this Agreement, and will disclose the Confidential Information of Discloser only to the employees or contractors of Recipient who have a need to know such Confidential Information for purposes of this Agreement and who are under a duty of confidentiality no less restrictive than Recipient's duty hereunder. Recipient will protect Confidential Information from unauthorized use, access, or disclosure in the same manner as Recipient protects its own confidential or proprietary information of a similar nature but with no less than reasonable care.

10.3 Exceptions. Recipient's obligations under Section 10.2 with respect to any Confidential Information will terminate if Recipient can show by written records that such information: (a) was already known to Recipient at the time of disclosure by Discloser; (b) was disclosed to Recipient by a third party who had the right to make such disclosure without any confidentiality restrictions; (c) is, or through no fault of Recipient has become, generally available to the public; or (d) was independently developed by Recipient without access to, or use of, Discloser's Information. In addition, Recipient will be allowed to disclose Confidential Information to the extent that such disclosure is required by law or by the order of a court of similar judicial or administrative body, provided that Recipient notifies Discloser of such required disclosure promptly and in writing and cooperates with Discloser, at Discloser's request and expense, in any lawful action to contest or limit the scope of such required disclosure.

11. GENERAL

11.1 Assignment. This Agreement and any Orders, and any of Your rights or obligations thereunder, may not be assigned, subcontracted or transferred by You, in whole or in part, whether voluntary, by operation of contract, law or otherwise, without the prior written consent of VMware. Any attempted assignment or transfer in violation of the foregoing will be null and void. Subject to the foregoing, this Agreement will be binding upon and will inure to the benefit of the parties and their respective successors and assigns.

11.2 Notices. Any notice delivered by VMware to You under this Agreement will be delivered via mail, email or fax.

11.3 Waiver. The waiver of a breach of any provision of this Agreement shall not constitute a waiver of any other provision or any subsequent breach.

11.4 Severability. If any provision of this Agreement is held to be illegal, invalid or unenforceable, the provision will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remaining provisions of this Agreement will remain in full force and effect.

11.5 Compliance with Laws; Export Control; Government Regulations. Each party shall comply with all laws applicable to the actions contemplated by this Agreement. You acknowledge that the Hosted Service is of United States origin, is provided subject to the U.S. Export Administration Regulations, may be subject to the export control laws of the applicable territory, and that diversion contrary to applicable export control laws is prohibited. You represent that (1) You are not, and are not acting on behalf of, (a) any person who is a citizen, national, or resident of, or who is controlled by the government of any country to which the United States has prohibited export transactions; or (b) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List; and (2) You will not permit the Hosted Service to be used for, any purposes prohibited by law, including, any prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons. All VMware products, services (including but not limited to pre-packaged professional services offerings and Hosted Services) and publications are commercial in nature. The software, Hosted Services, publications and software documentation are "Commercial Items," as that term is defined in 48 C.F.R.§2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. §252.227-7014(a)(1) and 48 C.F.R. §252.227-7014(a)(5), and used in 48 C.F.R. §12.211, 48 C.F.R. §12.212 and 48 C.F.R. §227.7202, as applicable. Pursuant to 48 C.F.R. §12.211, 48 C.F.R. §12.212, 48 C.F.R.§252.227-7015, 48 C.F.R. §227.7202 through 227.7202-4, 48 C.F.R. §52.227-19 and other relevant sections of the Code of Federal Regulations, as applicable, VMware's publications, commercial computer software, Hosted Services and commercial computer software documentation are distributed and licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in the license agreements and terms of service that accompany the products and software documentation and the terms and conditions herein.

11.6 Construction. The headings of sections of this Agreement are for convenience and are not to be used in interpreting this Agreement. As used in this Agreement, the word 'including' means "including but not limited to."

11.7 Governing Law. This Agreement is governed by the laws of the State of California, United States of America, unless mandated by other law. The United Nations Convention for the International Sale of Goods shall not apply.

11.8 Third Party Rights. Other than as expressly set out in this Agreement, this Agreement does not create any rights for any person who is not a party to it, and no person who is not a party to this Agreement may enforce any of its terms or rely on any exclusion or limitation contained in it.

11.9 Order of Precedence. In the event of conflict or inconsistency among this Agreement and the Order, the following order of precedence shall apply: (a) this Agreement and (b) the Order. The terms of this Agreement shall supersede and control over any conflicting or additional terms and conditions of any Order acknowledgement or confirmation or other document issued by You, unless the parties execute a written agreement expressly indicating: (i) that such Order

shall modify this Agreement; or (ii) that the terms of such Order shall supersede and control in the event of any inconsistency.

11.10 Entire Agreement. This Agreement, including accepted Orders and any amendments hereto, contains the entire agreement of the parties with respect to the subject matter of this Agreement and supersedes all previous or contemporaneous communications, representations, proposals, commitments, understandings and agreements, whether written or oral, between the parties regarding the subject matter hereof. This Agreement may be amended only in writing signed by authorized representatives of both parties.

11.11 Contact Information. Please direct legal notices or other correspondence to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America. If You have any questions concerning this Agreement, please send an email to info@vmware.com.

12. Hosted Service-Specific Terms And Conditions. In addition to the above sections, the Hosted Service is subject to the following terms and conditions. In the event of any conflict between the Hosted Service-specific terms and conditions and Sections 1-11 of this Agreement, the Hosted Service-specific terms and conditions shall control.

Socialcast SaaS
Socialcast Dedicated Cloud

" **Content**" means the audio and visual information, documents, software, products and services contained in or made available to You in the course of using the Hosted Service.

" **Named User**" means a designated user who can access or use the Hosted Service.

" **Private Group**" means a portion of the Hosted Service that can be accessed only after receipt and acceptance of an invitation from You or a Named User.

" **External Contributor**" means an individual who is not a "Named User" but is authorized by You to access and post information to one or more Private Groups but is otherwise prohibited from accessing or using the Hosted Service.

" **Hosted Service**" means the VMware hosted offering listed in VMware's commercial price list to which You acquire rights to access and use under an Order. The Hosted Service, includes, but is not limited to, Content.

" **Freemium Offering**" means the Hosted Service made available by VMware on a no-charge basis for up to a total of fifty (50) Named Users and External Contributors.

" **Named User**" means a designated user who can access or use the Hosted Service.

Subject to the terms and conditions of this Agreement and payment of all fees specified in the applicable Order(s), VMware grants to You, during the Hosted Service Subscription Term, a right to: (i) access and use the Hosted Service by the total number and type of Named Users set forth in the applicable Order and (ii) permit External Contributors to access and use Private Groups.

If You have a total of fifty (50) or fewer Named Users and External Contributors, VMware grants to You a right to access and use the Freemium Offering by the Named Users and External Contributors until either You or VMware terminate such right by providing written notice of termination to the other.

You, not VMware, are solely responsible for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use of all Customer Data, and VMware shall not be responsible or liable for the deletion, correction, destruction, damage, loss or failure to store any Customer Data. Upon the expiration of the Hosted Service Subscription Term, this Agreement will automatically renew, at VMware's then current fees, for successive terms. The length of each renewal term shall be one (1) year, unless otherwise specified in the associated renewal Order. Each renewal term shall be considered a new Hosted Service Subscription Term. Either VMware or You may terminate this Agreement, without cause, or reduce the number of licenses, effective only upon the expiration of the then current Hosted Subscription Term, by notifying the other in writing at least thirty (30) days prior to the expiration of the then current Hosted Service Subscription Term. In the event this Agreement is terminated (other than by reason of Your breach), VMware will make available to You, within 30 days of termination of the Agreement, a file of any Customer Data stored by VMware, if You so request at the time of such termination. VMware does not have any obligation to retain Customer Data, and may delete Customer Data, more than thirty (30) days after any termination of this Agreement.

VMware reserves the right to withhold, remove and/or discard Customer Data, without notice, upon any breach of this Agreement by You. Upon termination of Your access to the Hosted Service or this Agreement for cause, Your right to access or use Customer Data immediately ceases, and VMware shall have no obligation to maintain or to make available or provide to You any Customer Data. VMware shall have the right, but not the obligation, to monitor Customer Data, including chat rooms and forums, and Your use of the Hosted Service to determine compliance with this Agreement and any operating rules established by VMware, to provide support to You and to satisfy any law, regulation or authorized government request. VMware shall have the right in its sole discretion to edit, refuse to post or remove any material submitted to or posted using the Hosted Service. Without limiting the foregoing, VMware shall have the right to remove any material that VMware in its sole discretion, finds to be in violation of the provisions of this Agreement.

VMware may collect certain data and information as a result of Your access or use of the Hosted Service. VMware may share personal information of Yours and the Named Users with its service providers and suppliers to the extent needed to deliver or provide information on products or services or otherwise support Your business needs relating to the Hosted Service. Third party service providers and suppliers receiving any such personal information are expected to apply the same level of privacy protection as VMware. They are required to keep confidential the personal information received from VMware and may not use it for any purpose other than those set forth above.

VMware may reference You as a customer of VMware, which may include a copy of Your corporate logo, unless You provide prior written notice to VMware prohibiting such reference.

In addition to this Agreement, the Hosted Service shall be subject to the terms and conditions of the Socialcast Service Level Agreement.

NOTWITHSTANDING ANY OTHER PROVISION IN THIS AGREEMENT, THE FREEMIUM OFFERING IS PROVIDED "AS-IS" WITHOUT INDEMNIFICATION, SUPPORT OR WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED.

Copyright © 1998-2016

VMware, Inc. All rights reserved. VMware software products are protected by one or more U.S. Patent Numbers

D617,808, D617,809, D617,810, D617,811, 6,256,637, 6,360,219, 6,397,242, 6,496,847, 6,567,905, 6,681,226, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,883,095, 6,940,980, 6,944,699, 6,961,806, 6,961,941, 6,970,562, 7,017,041, 7,055,032, 7,065,642, 7,069,413, 7,069,435, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149,310, 7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999,

7,278,030, 7,281,102, 7,290,253, 7,343,599, 7,356,679, 7,373,355, 7,386,720, 7,409,487, 7,412,492, 7,412,702, 7,424,710, 7,428,636, 7,433,951, 7,434,002, 7,447,854, 7,447,903, 7,467,067, 7,475,002, 7,478,173, 7,478,180, 7,478,218, 7,478,3[illegible]3, 7,487,314, 7,490,216, 7,500,048, 7,506,122, 7,516,453, 7,529,897, 7,555,747, 7,565,527, 7,571,471, 7,577,722, 7,581,064, 7,590,715, 7,590,982, 7,594,111, 7,596,594, 7,596,697, 7,599,493, 7,603,704, 7,606,868, 7,620,523, 7,620,766, 7,620,955, 7,624,240, 7,630,493, 7,636,831, 7,657,659, 7,657,937, 7,665,088, 7,672,814, 7,680,919, 7,693,996, 7,694,101, 7,702,843, 7,707,185, 7,707,285, 7,707,578, 7,716,446, 7,734,045, 7,734,911, 7,734,912, 7,735,136, 7,743,389, 7,761,917, 7,765,543, 7,774,391, 7,779,091, 7,783,779, 7,783,838, 7,793,279, 7,797,748, 7,801,703, 7,802,000, 7,802,248, 7,805,676, 7,814,495, 7,823,145, 7,831,661, 7,831,739, 7,831,761, 7,831,773, 7,840,790, 7,840,839, 7,840,993, 7,844,954, 7,849,098, 7,853,744, 7,853,960, 7,856,419, 7,856,531, 7,856,637, 7,865,663, 7,869,967, 7,886,127, 7,886,148, 7,886,346, 7,890,754, 7,895,437, 7,908,646, 7,912,951, 7,921,197, 7,925,850, 7,933,981, 7,934,017, 7,934,020, 7,941,470, 7,941,827, 7,945,436, 7,945,761, 7,945,908, 7,945,958, 7,953,833, 7,958,558, 7,962,647, 7,966,615, 7,970,938, 7,971,015, 7,971,047, 7,971,182, 7,975,165, 7,984,254, 7,984,264, 7,984,304, 8,001,083, 8,001,322, 8,006,043, 8,010,667, 8,010,676, 8,010,701, 8,013,859, 8,015,367, 8,015,388, 8,019,861, 8,024,506, 8,024,779, 8,028,071, 8,037,032, 8,037,227, 8,037,280, 8,046,468, 8,056,076, 8,060,342, 8,060,722, 8,060,875, 8,060,877, 8,060,883, 8,069,250, 8,074,045, 8,086,822, 8,095,525, 8,095,929, 8,095,931, 8,099,568, 8,099,607, 8,112,505, 8,117,410, 8,127,014, 8,127,107, 8,127,301, 8,141,075, 8,141,163, 8,145,752, 8,145,763, 8,145,836, 8,146,082, 8,151,263, 8,166,107, 8,166,211, 8,166,253, 8,166,349, 8,166,474, 8,166,475, 8,166,554, 8,170,123, 8,171,033, 8,171,140, 8,171,141, 8,171,142, 8,171,278, 8,171,338, 8,171,345, 8,171,482, 8,171,485, 8,171,488, 8,171,548, 8,176,493, 8,195,774, 8,195,866, 8,201,169, 8,204,986, 8,209,343, 8,209,408, 8,209,680, 8,213,608, 8,214,522, 8,214,576, 8,214,802, 8,214,875, 8,219,063, 8,219,779, 8,219,987, 8,225,071, 8,233,882, 8,234,518, 8,239,608, 8,239,646, 8,239,655, 8,244,853, 8,245,081, 8,245,129, 8,245,227, 8,250,197, 8,250,214, 8,250,519, 8,250,586, 8,250,638, 8,255,484, 8,255,806, 8,260,816, 8,260,904, 8,261,265, 8,266,099, 8,266,275, 8,266,279, 8,266,395, 8,266,404, 8,266,628, 8,271,450, 8,275,563, 8,281,318, 8,281,377, 8,286,174, 8,291,135, 8,291,159, 8,291,180, 8,291,436, 8,295,308, 8,296,472, 8,296,551, 8,296,759, 8,296,767, 8,301,874, 8,302,094, 8,307,187, 8,307,191, 8,307,192, 8,312,175, 8,312,471, 8,312,522, 8,316,193, 8,316,374, 8,321,643, 8,321,842, 8,321,850, 8,327,059, 8,332,921, 8,335,703, 8,336,049, 8,340,287, 8,341,749, 8,347,263, 8,347,344, 8,352,240, 8,352,482, 8,352,490, 8,352,705, 8,352,944, 8,359,374, 8,359,422, 8,359,451, 8,359,593, 8,364,932, 8,380,747, 8,380,939, 8,392,361, 8,392,838, 8,397,038, 8,402,224, 8,402,441, 8,402,527, 8,407,475, 8,407,518, 8,412,910, 8,417,812, 8,429,647, 8,429,665, 8,438,430, 8,441,494, 8,443,139, 8,443,156, 8,443,166, 8,443,261, 8,443,367, 8,448,022, 8,453,108, 8,453,143, 8,458,318, 8,458,329, 8,463,730, 8,463,905, 8,464,022, 8,464,259, 8,468,310, 8,473,946, 8,473,947, 8,478,725, 8,478,801, 8,478,924, 8,479,195, 8,543,781, 8,543,790, 8,544,010, 8,484,405, 8,489,636, 8,489,699, 8,489,719, 8,489,800, 8,490,085, 8,495,631, 8,498,987, 8,499,004, 8,499,297, 8,510,438, 8,510,590, 8,510,827, 8,521,504, 8,521,686, 8,521,666, 8,522,228, 8,527,673, 8,528,107, 8,533,382, 8,553,745, 8,543,781, 8,543,790, 8,544,010, 8,549,241, 8,549,364, 8,554,900, 8,554,981, 8,555,003, 8,555,081, 8,555,274, 8,560,577, 8,560,626, 8,560,747, 8,560,791, 8,561,061, 8,566,502, 8,566,744, 8,572,606, 8,572,608, 8,577,853, 8,577,937, 8,578,083, 8,578,380, 8, 583,875, 8,584,126, 8,589,913, 8,589,940, 8,595,369, 8,595,460, 8,595,487, 8,595,824, 8,607,011, 8,607,013, 8,612,659, 8,615,489, 8,619,771, 8,621,136, 8,621,607, 8,626,723, 8,631,065, 8,631,066, 8,631,117, 8,631,403, 8,635,330, 8,635,395, 8635,493, 8,639,917, 8,640,126, 8,650,359, 8,650,566, 8,650,564, 8,656,000, 8,655,971, 8,656,222, 8,656,389, 8,656,497, 8,661,182, 8,661,213, 8,661,428, 8,666,938, 8,667,187, 8,667,459, 8,667,500, 8,671,238, 8,677,085, 8,667,187, 8,677,351, 8,667,352, 8,683,041, 8,683,466, 8,688,823, 8,694,713, 8,694,728, 8,694,746 8,694,828, 8,700,585, 8,700,611, 8,701,107, 8,706,991, 8,707,035, 8,712,960, 8,713,273, 8,713,646, 8,717,895, 8,718,070, 8,719,401, 8,719,513, 8,719,545, 8,719,661, 8,719,800, 8,719,817, 8,719,823, 8,724,696, 8,725,886, 8,726,273, 8,726,225, 8,732,313, 8,732,700, 8,738,333, 8,738,868, 8,743,888, 8,743,889, 8,745,236, 8,745,241, 8,745,308, 8,745,336, 8,745,351, 8,750,119, 8,750,164, 8,751,867, 8,752,058, 8,756,397, 8,756,426, 8,763,115, 8,761,036, 8,762,660, 8,762,684, 8,769,174, 8,769,184, 8,775,594, 8,775,696, 8,775,748, 8,775,773, 8,775,774, 8,775,815, 8,775,903, 8,776,055, 8,776,089, 8,782,242, 8,782,310, 8,782,768, 8,788,079, 8,789,049, 8,793,428, 8,798,541, 8,799,418, 8,799,897, 8,799,921, 8,880,018, 8,805,934, 8,806,217, 8,806,484, 8,812,876, 8,813,074, 8,819,357, 8,817,620, 8,817,621, 8,819,674, 8,819,676, 8,819,822, 8,825,851, 8,825,909, 8,826,273, 8,826,278, 8,826,283, 8,826,289, 8,826,432, 8,825,994, 8,830,823, 8,830, 8,358,832,351, 8,832,390, 8,832,682, 8,832,785, 8,837,493, 8,839,201, 8,839,202, 8,839,266, 8,839,914, 8,838,756, 8,842,679, 8,843,933, 8,843,935, 8,850,004, 8,856,784, 8,862,695, 8,862,868, 8,863,127, 8,868,610, 8,868,880, 8,869,139, 8,874,744, 8,874,859, 8,875,162, 8,875,266, 8,875,288, 8,874,802, 8,874,803, 8,880,468, 8,880,470, 8,880,774, 8,880,930, 8,881,143, 8,886,708, 8,886,865, 8,892,737, 8,892,706, 8,892,776, 8,893,261, 8,892,716, 8,892,706, 8,892,716, 8,892,737, 8,892,776, 8,893,261, 8,898,108, 8,898,676, 8,898,508, 8,898,509, 8,898,518, 8,902,248, 8,902,242, 8,904,081, 8,910,297, 8,909,602, 8,909,928, 8,910,161, 8,910,228, 8,913,483, 8,913,611, 8,914,013, 8,914,567, 8,914,575, 8,914,598, 8,914,610, 8,914,684, 8,914,730, 8,917,617, 8,924,524, 8,924,534, 8,924,608, 8,924,967, 8,924,970, 8,925,036, 8,929,287, 8,930,592, 8,930,812, 8,930,948, 8,935,429, 8,935,456, 8,935,500, 8,938,680, 8,943,259, 8,943,296, 8,949,295, 8,949,399, 8,949,531, 8,949,546, 8,949,570, 8,949,585, 8,949,731, 8,949,791, 8,849,794, 8,949,817, 8,954,050, 8,954,387, 8,954,545, 8,954,575, 8,954,665, 8,955,072, 8,955,151, 8,958,292, 8,958,298, 8,959,215, 8,959,312, 8,959,338, 8,959,529, 8,964,528, 8,964,598, 8,964,767, 8,966,024, 8,966,029, 8,966,035, 8,966,040, 8,966,479, 8,966,581, 8,966,623, 8,972,981, 8,977,702, 8,977,736, 8,978,053, 8,978,110, 8,983,988, 8,984,508, 8,990,531, 8,990,699, 8,995,763, 8,996,853, 8,996,884, 8,997,187, 9,003,027, 9,003,037, 9,007,903, 9,008,087, 9,009,219, 9,009,727, 9,007,903, 9,008,087, 9,009,727, 9,015,180, 9,015,203, 9,015,823, 9,019,826, 9,019,977, 9,021,037, 9,026,510, 9,026,613, 9,026,630, 9,027,003, 9,027,031, 9,031,894, 9,032,050, 9,032,133, 9,032,170, 9,032,176, 9,032,181, 9,032,398, 9,032,402, 9,032,425, 9,037,522, 9,037,556, 9,037,621, 9,037,689, 9,037,719, 9,037,758, 9,037,873, 9,038,066, 9,042,304, 9,043,452, 9,043,792, 9,047,083, 9,047,087, 9,047,133, 9,049,153, 9,049,193, 9,049,257, 9,052,825, 9,052,937, 9,052,949, 9,052,961, 9,052,967, 9,053,064, 9,053,065, 9,054,995, 9,055,119, 9,058,232, 9,058,259, 9,058,353, 9,058,420, 9,058,495, 9,059,964, 9,059,989, 9,059,999, 9,063,756, 9,063,762, 9,063,766, 9,063,768, 9,063,866, 9,064,447, 9,069,579, 9,069,600, 9,069,607, 9,069,608, 9,069,902 , 9,075,718, 9,075,731, 9,077,664, 9,077,725, 9,081,536, 9,081,622, 9,081,686, 9,081,722, 9,083,606, 9,086,904, 9,086,921, 9,086,981, 9,087,191, 9,088,591, 9,092,318, 9,094,413, 9,097,528, 9,098,318, 9,098,347, 9,098,457, 9,099,974, 9,100,293, 9,104,402, 9,104, 469, 9,106,587, 9,116,726, 9,116,829, 9,116,737, 9,116,903, 9,122,594, 9,122,765, 9,123,031, 9,124,488, 9,124,538, 9,128,746, 9,129,062, 9,130,821, 9,130,879, 9,134,922, 9,134,992, 9,135,050, 9,135,171, 9,135,287, 9,135,342, 9,135,457, 9,137,052, 9,137,107, 9,137,222, 9,141,444, 9,141,578, 9,142,004, 9,141,381, 9,146,712, 9,146,721, 9,146,758, 9,146,766, 9,146,841, 9,146,847, 9,148,416, 9,152,445, 9,152,448, 9,152,548, 9,152,570, 9,152,572, 9,154,433, 9,158,434, 9,158,550, 9,158,561, 9,158,601, 9,158,665, 9,160,612, 9,160,630, 9,164,695, 9,166,895, 9,167,104, 9,170,798, 9,170,924, 9,171,139, 9,172,603, 9,172,663, 9,176,780, 9,177,250, 9,178,833, 9,182,927, 9,183,015, 9,183,016, 9,183,034, 9,183,093, 9,183,099, 9,183,101, 9,183,103, 9,183,151, 9,185,069, 9,185,099, 9,189,265, 9,189,410, 9,189,419, 9,189,513, 9,189,609, 9,189,622, 9,189,758, 9,191,384, 9,195,393, 9,195,487, 9,195,491, 9,195,518, 9,195,585, 9,195,707, 9,195,811, 9,197,529, 9,201,646, 9,201,653, 9,201,667, 9,201,674, 9,201,755, 9,202,025, 9,203,701, 9,203,703, 9,203,820, 9,208,015, 9,209,998, 9,210,079, 9,213,544, 9,213,556, 9,213,565, 9,213,570, 9,213,572, 9,213,651, 9,213,851,9,213,852, 9,213,859, 9,214,004, 9,215,177, 9,215,210, 9,215,213, 9,215,214, 9,218,140, 9,218,200, 9,219,813, 9,219,741, 9,223,608, 9,223,722, 9,223,767, 9,225,597, 9,225,638, 9,225,647, 9,225,742, 9,226,155, 9,229,754, 9,230,001, 9,231,818, 9,231,882, 9,231,891, 9,231,892, 9,235,577, 9,237,147, 9,239,682, 9,239,729, 9,239,731, 9,239,776, 9,239,841, 9,244,669, 9,244,717, 9,244,732, 9,244,742, 9,244,755, 9,244,903, 9,245,000, 9,246,833, 9,246,877, 9,246,918, 9,247,042, 9,247,432, 9,250,827, 9,250,854, 9,250,943, 9,251,102, 9,251,103, 9,235,109, 9,253,158, 9,253,309, 9,256,353, 9,256,515, 9,256,746, 9,257,092, 9,258,301, 9,258,359, 9,262,189, 9,262,192, 9,262,198, 9,262,214, 9,264,517, 9,262,750, 9,264,313, 9,264,330, 9,264,704, 9,268,549, 9,268,590, 9,268,591, 9,268,592, 9,268,610, 9,268,642, 9,268,836, 9,270,777, 9,274,814, 9,274,821, 9,274,834, 9,274,974, 9,275,245, 9,276,809, 9,276,897, 9,276,904, 9,277,237, 9,280,300, 9,280,358, 9,280,665, 9,282,019, D751,082, 9,285,993, 9,285,999, 9,286,095, 9,286,102, 9,288,081, 9,288,104, 9,288,259, 9,292,281, 9,292,353, 9,292,401, 9,292,416, 9,292,422, 9,292,452, 9,292,507, 9,292,699, 9,293,376, 9,294,407, 9,294,524, 9,298,375, 9,298,377, 9,298,490, 9,298,512, 9,298,538, 9,298,936, 9,300,593, 9,300,603, 9,304,662, 9,304,705, 9,304,803, 9,304,804, 9,304,873, 9,304,878, 9,304,915, 9,305,014, 9,306,843, 9,306,864, 9,306,909, 9,306,910, 9,306,875, 9,311,129, 9,311,140, 9,311,313, 9,311,464, 9,311,475, 9,313,129, 9,313,263, 9,317,207, 9,317,260, 9,317,315, 9,317,318, 9,317,326, 9,317,333, 9,317,387, 9,317,444, 9,319,288, 9,319,336, 9,319,337, 9,319,338, 9,319,375, 9,323,550, 9,323,565, 9,323,579, 9,325,713, D754,692, 9,329,855, 9,329,889, 9,329,894, 9,329,896, 9,329,958, 9,330,015, 9,330,424, 9,331,937, 9,331,938;patents pending.

Search

CONTACT SALES (/COMPANY/CONTACT_SALES.HTML) GET SUPPORT (/SUPPORT.HTML)
ABOUT VMWARE (/COMPANY.HTML) CAREERS (HTTPS://CAREERS.VMWARE.COM)

© 2017 VMware, Inc

Terms of Use (/help/legal.html)
Privacy (/help/privacy.html)
Accessibility (/help/accessibility.html)
Site Index (/site_index.html)
Trademarks (/help/trademarks.html)
Help (/help.html)
Feedback

(https://twitter.com/VMware) (https://www.facebook.com/vmware) (https://www.linkedin.com/company/vmware)
(http://www.youtube.com/user/vmwaretv) (https://plus.google.com/+vmware)

(/)

(/)

(/)

VMware Professional Services
General Terms & Conditions

1. Definitions.

a) "**Acceptance Period**" means a period of ten (10) business days (not including Federal or Bank Holidays) following, (i) with respect to a fixed fee engagement, delivery of the applicable Project Milestone Completion Form or (ii) with respect to time and materials engagements, the submission of timesheets.

b) "**Consulting Services**" means those services provided by VMware to Customer as described in this Statement of Work ("**SOW**"). Alternatively, if Customer ordered such services via a VMware online datasheet in lieu of a Statement of Work, all references herein to this SOW shall be deemed to refer to such datasheet.

c) "**Customer Materials**" means any materials or Technology provided to VMware by Customer in connection with the Consulting Services.

d) "**Deliverables**" means work product resulting from the Consulting Services, which includes VMware's Prior Technology.

e) "**Derivative Work**" means a derivative work as defined under applicable intellectual property laws.

f) "**Intellectual Property Rights**" means all worldwide intellectual property rights, including without limitation, copyrights, trademarks, service marks, trade secrets, know-how, inventions, patents, patent applications, moral rights and all other proprietary rights, whether registered or unregistered.

g) **"Parties"** means VMware and Customer collectively and a **"Party"** means VMware or Customer individually.

h) "**Prior Technology**" means any Technology that has been developed or otherwise created by or on behalf of VMware or licensed by VMware prior to or outside of this SOW, and which may be improved or modified in the course of developing the Deliverables.

i) "**Taxes**" means any sales, use and other taxes (other than taxes on VMware's income), export and import fees, customs duties and similar charges applicable to the transactions contemplated by this SOW that are imposed by any government or other authority.

j) "**Technology**" means algorithms, approaches, code, concepts, data, designs, developments, documentation, discoveries, expressions, inventions, know how, methodologies, multi-media files, object codes, processes, programs, skills, software, techniques, technology, templates, text, tools, and web pages.

2. Consulting Services.

a) Consulting Services. Subject to the terms and conditions set forth herein, VMware will provide the Consulting Services and Deliverables as specified in this SOW.

b) Acceptance**.**

i) With respect to fixed fee engagements, upon completion of each milestone, VMware will deliver to Customer a Project Milestone Completion Form. With respect to time and materials engagements, VMware will deliver timesheets to Customer. Customer will return the Project Milestone Completion Form or timesheets, as applicable, to VMware within the Acceptance Period, indicating thereon Customer's acceptance of the Deliverables or Consulting Services covered thereby.

ii) If Customer reasonably believes that VMware did not complete the Consulting Services and/or Deliverables in substantial conformance with this SOW, Customer will notify VMware within the Acceptance Period, in writing, of its rejection of the Consulting Services or Deliverables. Customer's notice must specifically identify and justify each non-conformance with the terms of this SOW. VMware will address Customer's issues and then re-present the Project Milestone Completion Form or timesheets for Customer's acceptance in accordance with the requirements of this Section 2.

iii) If VMware does not receive Customer's acceptance or rejection in the form set forth above within the Acceptance Period, the Consulting Services and Deliverables will be deemed accepted by Customer, and Customer will have waived any right of rejection.

c) Project Change Request.

i) Either Party may request a modification to an accepted Deliverable or to any material provision of an SOW by means of a Project Change Request ("**PCR**"). When a Party submits a PCR, VMware will promptly estimate the financial and schedule impacts, if any, that the proposed PCR would have. The Parties will promptly meet to review the estimate and to determine whether, and with what modifications, the PCR would be mutually acceptable. VMware may not unreasonably refuse to accept a PCR initiated by Customer, if Customer agrees to bear the financial and schedule impacts identified by VMware.

ii) If the Parties agree on the PCR, they will properly memorialize such agreement and the date thereof, and attach the final PCR to the SOW. If the Parties are unable to agree within five (5) days after the PCR is submitted, then the submitting Party may either withdraw the PCR or terminate the SOW with the only payments due being for Deliverables delivered, work performed, and expenses incurred by VMware prior to the termination date.

d) Customer Materials Delays. Customer acknowledges and agrees that VMware's performance of the Consulting Services and supply of the Deliverables is contingent on Customer's timely delivery of any Customer Materials required to perform the Consulting Services. As such, any reasonable scheduling and/or financial impacts caused by Customer's failure to deliver Customer Materials will be treated as a PCR.

e) Personnel. The personnel assigned to perform Consulting Services under an SOW will be determined solely by VMware. However, Customer may request, in writing, with specific reasons delineated, the replacement of VMware personnel or VMware contractors that Customer reasonably believes are not adequately performing the Consulting Services set forth in the SOW.

3. Intellectual Property.

a) Proprietary Rights. All Intellectual Property Rights in the Prior Technology and the Deliverables remain VMware property ("**VMware Proprietary Works**"). Notwithstanding the foregoing, all written reports, analyses and other working papers delivered by VMware to Customer as part of the Consulting Services ("**Document Work Product**"), subject to and exclusive of any Intellectual Property Rights embodied therein, will belong to Customer upon payment in full of all amounts payable by Customer pursuant to this SOW. Nothing herein precludes VMware from developing, using or marketing services or materials that are similar or related to the Deliverables.

b) Customer Materials. Any Customer Materials used by VMware in connection with this SOW remain Customer property. Customer warrants that it has the necessary rights to provide the Customer Materials to VMware for VMware to access, use and/or modify them as necessary for VMware's performance of the Consulting Services.

c) Deliverables License. Subject to Customer's payment in full for Deliverables, Customer is licensed to (a) use such Deliverables internally, for the sole purpose for which they were provided, on a perpetual, non-exclusive, non-transferable, without rights to sublicense, royalty-free, worldwide basis ("**Deliverables License**"), and (b) make, for internal use only, a reasonable number of copies of the original Document Work Product in amounts reasonably necessary for Customer's internal use. Customer shall not sublicense or otherwise transfer to any third party any Deliverable. Other than as specifically provided herein, Customer may not modify, alter, decompile, disassemble, reverse-engineer, or create Derivative Works from the Deliverables.

d) VMware License. Customer hereby grants to VMware a non-exclusive, worldwide, personal, royalty-free, non-transferable (except to entities controlling, controlled by, or under common control with VMware) license under Customer's Intellectual Property Rights in the Customer Materials solely to the extent necessary for VMware to use, make, copy, modify, and create Derivative Works of the Customer Materials for the purpose of providing the Consulting Services under this SOW. The term of such VMware license expires upon completion of the Consulting Services under this SOW.

4. Confidentiality.

a) Definition. "**Confidential Information**" means information or materials provided by one Party (**"Discloser"**) to the other Party (**"Recipient"**) which are in tangible form and labeled "confidential" or the like, or, information which a reasonable person knew or should have known to be confidential. The following information shall be considered Confidential Information whether or not so marked or identified: any personally identifiable information (such as the names of Discloser's customers or the physical address of any equipment) contained in any information collected about Discloser's computing environment, Discloser's business operations, pricing, discounts, source code, product roadmaps or strategic marketing plans.

b) Protection. Recipient may use Confidential Information of Discloser: (i) to exercise its rights and perform its obligations under this SOW; or (ii) in connection with the Parties' ongoing business relationship. Recipient shall not use any Confidential Information of Discloser for any purpose not expressly permitted by this SOW, and shall disclose the Confidential Information of Discloser only to the employees or contractors of Recipient who have a "need to know" such Confidential Information for purposes of this SOW and who are under a duty of confidentiality no less restrictive than Recipient's duty hereunder. Recipient will protect Discloser's Confidential Information from unauthorized use, access, or disclosure in the same manner as Recipient protects its own confidential or proprietary information of a similar nature but with no less than reasonable care.

c) Exceptions. Recipient's obligations under Section 4(b) with respect to any of Discloser's Confidential Information shall terminate if Recipient can show by written records that such information: (i) was already known to recipient at the time of disclosure by Discloser; (ii) was disclosed to Recipient by a third party who had the right to make such disclosure without any confidentiality restrictions; (iii) is, or through no fault of Recipient has become, generally available to the public; or (iv) was independently developed by Recipient without access to, or use of, Discloser's Confidential Information. In addition, Recipient will be allowed to disclose Discloser's Confidential Information to the extent that such disclosure is required by law or by the order of a court or similar judicial or administrative body, provided that Recipient notifies Discloser of such required disclosure promptly and in writing and cooperates with Discloser, at Discloser's request and expense, in any lawful action to contest or limit the scope of such required disclosure.

d) Permitted Disclosure. Notwithstanding anything to the contrary herein, neither Party shall disclose the terms and conditions of this SOW to any third party, without the prior written consent of the other Party. Notwithstanding the foregoing each Party may disclose the terms and conditions of this SOW without the prior written consent of the other Party: (i) as required by any court or other governmental body; (ii) as otherwise required by law; (iii) to legal counsel of the Parties; (iv) in confidence, to accountants, banks, and financing sources and their advisors; (v) in connection with the enforcement of this SOW or rights under this SOW; or (vi) in confidence, in connection with an actual or proposed merger, acquisition, or similar transaction.

5. Intellectual Property Indemnification.

a) Defense and Indemnification. Subject to the remainder of this Section 5, VMware shall defend Customer against any third party claim that the Deliverables and/or Prior Technology when used as contemplated by this SOW infringe any patent, trademark or copyright of such third party, or misappropriate a trade secret (but only to the extent that such misappropriation is not a result of Customer's actions) under the laws of: (a) the United States and Canada; (b) the European Economic Area; (c) Australia; (d) New Zealand; (e) Japan; or (f) the People's Republic of China, to the extent that such countries are part of the territory of use for the Deliverables License ("Infringement Claim"), and indemnify Customer from the resulting costs and damages finally awarded against Customer to such third party by a court of competent jurisdiction or agreed to in settlement; provided that Customer: (i) promptly provides VMware with notice of such Infringement Claim; (ii) allows VMware sole control over the defense thereof and related settlement negotiation; and (iii) reasonably cooperates in response to VMware requests for assistance. Customer may not settle or compromise any Infringement Claim without the prior written consent of VMware.

b) Remedies. Should the Deliverables and/or Prior Technology become, or in VMware's opinion be likely to become, the subject of an Infringement Claim, VMware will, at VMware's option and expense, either: (a) procure the rights necessary for Customer to make continued use of the affected Deliverables and/or Prior Technology in accordance with this SOW; (b) replace or modify the affected Deliverables and/or Prior Technology to make it non-infringing; or (c) terminate the Deliverables License to the affected Deliverables and/or Prior Technology, and, upon Customer's certified deletion or destruction of the affected Deliverables and/or Prior Technology, refund the fees paid by Customer for the applicable Consulting Services. Nothing in this Section 5(b) shall limit VMware's obligation under Section 5(a) to defend and indemnify Customer, provided that Customer replaces the allegedly infringing Deliverables and/or Prior Technology upon VMware's making alternate Deliverables or Prior Technology available to Customer and/or Customer discontinues using the allegedly infringing Deliverables and/or Prior Technology upon receiving VMware's notice terminating the affected Deliverables License.

c) Exclusions. Notwithstanding the foregoing, VMware will have no obligation under this Section 5 or otherwise with respect to any claim based on: (a) a combination of the Deliverables and/or Prior Technology with non-VMware products (other than non-VMware products that are listed on the purchase order and used in an unmodified form); (b) use for a purpose or in a manner for which the Deliverables and/or Prior Technology was not designed; (c) use of any older version of VMware software when use of a newer VMware revision would have avoided the infringement; (d) any modification to the Deliverables and/or Prior Technology made without VMware's express written approval; (e) any Deliverables and/or Prior Technology provided by VMware in accordance with Customer's specifications or designs; (f) any claim that relates to open source software or freeware technology or any derivatives or other adaptations thereof that is not embedded by VMware into VMware software listed on VMware's commercial price list or into Deliverables and/or Prior Technology; (g) any claim that relates to Linux or Android open source software, even when such open source software has been embedded into or distributed the Deliverables and/or Prior Technology; or (h) Customer materials or Technology that Customer instructs VMware to develop in a specific way or to achieve a specific end result. THIS SECTION 5 STATES CUSTOMER'S SOLE AND EXCLUSIVE REMEDY AND VMWARE'S ENTIRE LIABILITY FOR ANY INFRINGEMENT CLAIMS OR ACTIONS.

6. Warranties and Limitation of Liability.

a) VMware Warranty. VMware warrants that the Consulting Services to be performed hereunder will be done in a workmanlike manner in accordance with the standards of the industry. Customer must notify VMware of any failure to so perform before the end of the Acceptance Period. VMware's entire liability and Customer's sole remedy for VMware's failure to so perform shall be for VMware to, at its option, (i) use reasonable efforts to correct such failure, and/or (ii) terminate this SOW and refund that portion of any fees received that correspond to such failure to perform.

b) Disclaimer of Warranties. THE EXPRESS WARRANTIES SET FORTH IN SECTION 6(a) ABOVE ARE IN LIEU OF ALL OTHER WARRANTIES, AND, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VMWARE DISCLAIMS, ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE REGARDING OR RELATING TO THE CONSULTING SERVICES OR DELIVERABLES, INCLUDING BUT NOT LIMITED TO THE DOCUMENT WORK PRODUCT, OR ANY OTHER MATERIALS FURNISHED OR PROVIDED TO CUSTOMER UNDER THIS SOW. VMWARE WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER BY VMWARE. NO EMPLOYEE, AGENT, REPRESENTATIVE OR AFFILIATE OF VMWARE HAS THE AUTHORITY TO BIND VMWARE TO ANY REPRESENTATIONS OR WARRANTIES OUTSIDE OF THESE GENERAL TERMS AND CONDITIONS.

c) Limitation of Liability. VMware shall not be liable for any incidental, consequential, exemplary, special or indirect damages (including, but not limited to, loss of profits, revenues, data and/or use), even if advised of the possibility thereof, under this SOW. VMware's total liability under this SOW shall not exceed the fees paid for the Consulting Services and Deliverables provided by VMware under this SOW. Customer may not bring a claim under this SOW more than eighteen (18) months after the cause of action arises.

7. Fees and Payment.

a) Payment. VMware will provide the Consulting Services as outlined in this SOW for i) a fixed fee or ii) on a time and materials basis as described in this SOW, plus applicable taxes and travel expenses in accordance with VMware's travel and expense policy (unless travel expenses are expressly included in the fixed fee or fees for consultants' time). Invoicing occurs upon Customer acceptance of each milestone or timesheet (as is applicable), or approval of travel expenses, and must be paid by Customer within thirty (30) days of the date of invoice. In the event Customer uses pre-purchased VMware Consulting and Training Credits as means of payment, upon acceptance of Project Milestone Completion Form(s), timesheets, or travel expenses, the VMware Consulting & Training Credits will be deducted from the Customer's balance. It shall be the Customer's responsibility to ensure that its purchase order ("**PO**") issued to VMware for the Consulting Services reflects the pricing set forth in this SOW. Once a PO from Customer has been fulfilled by VMware, VMware shall have no liability for any pricing in Customer's PO that is inconsistent with the pricing set forth in this SOW. Customer agrees that POs do not have to be signed to be valid and enforceable. Subject to these General Terms & Conditions, all fees are non-refundable.

b) Taxes**.** Fees are exclusive of Taxes, and Customer shall pay or reimburse VMware for all Taxes arising out of this SOW or the transactions contemplated by this SOW. If Customer is required to pay or withhold any Tax in respect of any payments due to VMware hereunder, Customer shall gross up payments actually made such that VMware shall receive sums due hereunder in full and free of any deduction for any such Tax. Customer confirms that VMware can rely on the Customer address set forth in this SOW as being the place of supply for tax purposes.

c) Late Payments**.** All amounts not paid when due shall incur a late charge equal to the lesser of one and one-half percent (1.5%) per month, or, the maximum amount allowed by applicable law. VMware may suspend provision of the Consulting Services while any payment is delinquent.

d) Currency. All charges and fees provided for in this SOW shall be in the currency specified in this SOW.

e) Canceling/Rescheduling SOW before Commencement. A minimum of fifteen (15) business days' written notice is required for rescheduling or canceling this SOW prior to the commencement of the Consulting Services. Only incurred expenses (e.g., airfare) will be owed and invoiced if said notice is given. The entire payment and incurred expenses are owed if this SOW is canceled with less than said notice.

8. Term and Termination.

a) Term. Subject to the Parties' respective termination rights hereunder, this SOW will be in full force and effect until (i) Customer's acceptance of the final Deliverable or final timesheet, or (ii) VMware and Customer mutually terminate this SOW in writing.

b) Termination. Either Party may terminate the SOW immediately upon written notice if: (i) the other Party breaches any provision of the SOW and does not cure the breach within

thirty (30) days after receiving written notice thereof from the other Party; or (ii) the other Party commits a material breach of the SOW. VMware may terminate the SOW in its entirety effective immediately upon written notice to Customer if Customer: (i) terminates or suspends its business; (ii) becomes insolvent, admits in writing its inability to pay its debts as they mature, makes an assignment for the benefit of creditors, or becomes subject to control of a trustee, receiver or similar authority; or (iii) becomes subject to any bankruptcy or insolvency proceeding.

c) Survival. Sections 1 (Definitions), 3 (Intellectual Property), 4 (Confidentiality), 6 (Warranties and Limitation of Liability), 8 (Term and Termination), and 9 (Miscellaneous) will survive termination or expiration of this SOW.

9. Miscellaneous.

a) Insurance. VMware will, at its sole cost and expense for the term of this SOW, carry general and professional liability, automobile, and workers compensation insurance, for claims for personal injury (including death) or damage to tangible or real property, which may arise or result from VMware's performance under this SOW. VMware will provide Customer with its then-current Memorandum of Insurance upon reasonable request.

b) Workplace Health and Safety. Customer must comply with all applicable laws relating to the health, safety and welfare of all VMware employees and contractors while they are on Customer premises in connection with the provision of Consulting Services.

c) Non-solicitation**.** Each Party agrees any individual who has received Confidential Information of the other Party shall not intentionally solicit for employment the employees or contractors of the other Party who are directly involved in the performance of this SOW hereunder for a period of twelve (12) months following such person's last involvement in the performance of this SOW hereunder. Both Parties acknowledge that (i) any newspaper or other public solicitation not directed specifically to such person shall not be deemed to be a solicitation for purposes of this provision, and (ii) this provision is not intended to limit the mobility of either Party's employees or contractors.

d) No Assignment. This SOW and any rights or obligations of Customer under it may not be assigned, subcontracted or otherwise transferred by Customer, in whole or in part, whether voluntary, by operation of contract, law or otherwise, without the prior written consent of VMware. . Any attempted assignment or transfer in violation of the foregoing will be null and void. VMware may assign this SOW, without consent, to any successor to all or substantially all its business or assets to which this SOW relates, whether by merger, sale of assets, sale of stock, reorganization or otherwise subject to the foregoing, this SOW will be binding upon and will inure to the benefit of the Parties and their respective successors and assigns.

e) Independent Contractors. The Parties are independent contractors. Nothing in this SOW shall be construed to create a partnership, joint venture or agency relationship between the Parties

f) Customer Warranties. Customer shall make no representations or warranties on behalf of VMware with respect to the Consulting Services and/or Deliverables.

g) Governing Law**.** This SOW is governed by the laws of the State of California and the United States of America, excluding its conflict of law principles. The Parties hereby consent to the exclusive jurisdiction of the state and federal courts located in Santa Clara County, California.

h) Force Majeure. Neither Party shall be liable to the other Party for its failure to perform any of its obligations under this SOW (except for breaches of Section 4 or any payment obligations) during any period in which such performance is delayed or rendered impracticable or impossible due to circumstances beyond the nonperforming Party's reasonable control.

i) Compliance with Laws; Export Control; Government Regulations. Each Party shall comply with all laws applicable to the actions contemplated by this SOW. Customer acknowledges that the Consulting Services, Deliverables, and any software provided to Customer hereunder are of United States origin and are provided subject to the U.S. Export Administration Regulations, may be subject to the export control laws of the applicable territory, and that diversion contrary to applicable export control laws is prohibited. Customer represents that (1) Customer is not, and is not acting on behalf of, (a) any person who is a citizen, national, or resident of, or who is controlled by the government of any country to which the United States has prohibited export transactions or (b) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List; and (2) Customer will not permit the Consulting Services, Deliverables, and software to be used for, any purposes prohibited by law, including any prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons.

j) End User License Agreement. If the Consulting Services involve VMware software products licensed to Customer under a separate license agreement, unless otherwise provided herein, the terms set out in such separate license agreement will apply with respect to each such VMware software product.

k) Acknowledgment. Unless otherwise stated in this SOW, Customer acknowledges that the Consulting Services set forth in this SOW do not include significant production, modification or customization of VMware licensed software.

l) Waiver. The waiver of a breach of any provision of this SOW shall not constitute a waiver of any other provision or any subsequent breach.

m) Publicity. VMware may reference Customer as a customer of VMware, subject to Customer's trademark and logo usage guidelines provided by Customer. Customer may reference VMware as a vendor of Customer and/or Customer's "architect of record" on the Deliverable, subject to VMware's trademark and logo usage guidelines, which can be obtained by contacting VMware's brand team at brand@vmware.com.

n) Counterparts. Facsimile, scanned or electronic signatures on this SOW shall legally bind the Parties to the same extent as originals. For purposes of this provision, "electronic signature" shall mean the representation of a signature that is applied to the agreement electronically. This SOW may be executed in multiple counterparts all of which taken together shall constitute one single agreement between the Parties.

o) Severability. If any provision in this SOW is held to be illegal, invalid, or unenforceable, the provision will be enforced to the maximum extent possible so as to effect the intent of the parties, and the remaining provisions of this SOW will remain in full force and effect.

p) Construction**.** The headings of sections of this SOW are for convenience and are not to be used in interpreting this SOW. As used in this SOW, the word "including" means "including but not limited to."

q) Notices. Unless otherwise set forth in this SOW, any notice regarding this SOW or required by law must be in writing and delivered to the other Party's legal department at the address listed below via: (a) personal delivery confirmed in writing by the recipient; (b) certified or registered mail; or (c) pre-paid commercial courier. Notices shall be deemed received upon the date of delivery shown by the corresponding confirmation. Either Party may change its address by notice to the other Party. All notices shall be directed to Customer to the address set forth in the SOW, and to VMware as follows: VMware, Inc., 3401 Hillview Ave., Palo Alto CA 94304, Attention: Legal Department.

r) Entire Agreement. This SOW (including the Exhibits) contains the entire agreement between the Parties with respect to the subject matter hereof and supersedes all previous or contemporaneous communications, representations, proposals, commitments, understandings and agreements, whether oral or written, between the Parties regarding the subject matter hereof. This SOW may be amended only in writing signed by authorized representatives of both Parties. No terms, provisions or conditions of any purchase order, acknowledgment or other business form that Customer may issue to VMware in connection with this SOW will have any effect on, or otherwise modify, the rights, duties or obligations of the Parties under this SOW, regardless of any failure of VMware to object to such terms, provisions or conditions. VMware hereby rejects any such additional or conflicting terms and conditions on any Customer purchase order, acknowledgement or other business form, unless expressly otherwise agreed to by the Parties in writing.

Attachment A, Exhibit 1

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls that party, and here "control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of that entity.

1.2 "Documentation" means that documentation that is generally provided to You by VMware with the Software, as revised by VMware from time to time, and which may include end user manuals, operation instructions, installation guides, release notes, and on-line help files regarding the use of the Software.

1.3 "Guest Operating Systems" means instances of third-party operating systems licensed by You, installed in a Virtual Machine and run using the Software.

1.4 "Intellectual Property Rights" means all worldwide intellectual property rights, including without limitation, copyrights, trademarks, service marks, trade secrets, know how, inventions, patents, patent applications, moral rights and all other proprietary rights, whether registered or unregistered.

1.5 "License" means a license granted under Section 2.1 (General License Grant).

1.6 "License Key" means a serial number that enables You to activate and use the Software.

1.7 "License Term" means the duration of a License as specified in the Order.

1.8 "License Type" means the type of License applicable to the Software, as more fully described in the Order.

1.9 "Open Source Software" or "OSS" means software components embedded in the Software and provided under separate license terms, which can be found either in the open_source_licenses.txt file (or similar file) provided within the Software or at www.vmware.com/download/open_source.html.

1.10 "Order" means a purchase order, enterprise license agreement, or other ordering document issued by You to VMware or a VMware authorized reseller that references and incorporates this EULA and is accepted by VMware as set forth in Section 4 (Order).

1.11 "Product Guide" means the current version of the VMware Product Guide at the time of Your Order, copies of which are found at www.vmware.com/download/eula.

1.12 "Support Services Terms" means VMware's then-current support policies, copies of which are posted at www.vmware.com/support/policies.

1.13 "Software" means the VMware Tools and the VMware computer programs listed on VMware's commercial price list to which You acquire a license under an Order, together with any software code relating to the foregoing that is provided to You pursuant to a support and subscription service contract and that is not subject to a separate license agreement.

1.14 "Territory" means the country or countries in which You have been invoiced; provided, however, that if You have been invoiced within any of the European Economic Area member states, You may deploy the corresponding Software throughout the European Economic Area.

1.15 "Third Party Agent" means a third party delivering information technology services to You pursuant to a written contract with You.

1.16 "Virtual Machine" means a software container that can run its own operating system and execute applications like a physical machine.

1.17 "VMware" means VMware, Inc., a Delaware corporation, if You are purchasing Licenses or services for use in the United States and VMware International Limited, a company organized and existing under the laws of Ireland, for all other purchases.

1.18 "VMware Tools" means the suite of utilities and drivers, Licensed by VMware under the "VMware Tools" name, that can be installed in a Guest Operating System to enhance the performance and functionality of a Guest Operating System when running in a Virtual Machine.

2. LICENSE GRANT.

2.1 General License Grant. VMware grants to You a non-exclusive, non-transferable (except as set forth in Section 12.1 (Transfers; Assignment) license to use the Software and the Documentation during the period of the license and within the Territory, solely for Your internal business operations, and subject to the provisions of the Product Guide. Unless otherwise indicated in the Order, licenses granted to You will be perpetual, will be for use of object code only, and will commence on either delivery of the physical media or the date You are notified of availability for electronic download.

2.2 Third Party Agents. Under the License granted to You in Section 2.1 (General License Grant) above, You may permit Your Third Party Agents to access, use and/or operate the Software on Your behalf for the sole purpose of delivering services to You, provided that You will be fully responsible for Your Third Party Agents' compliance with terms and conditions of this EULA and any breach of this EULA by a Third Party Agent shall be deemed to be a breach by You.

2.3 Copying Permitted. You may copy the Software and Documentation as necessary to install and run the quantity of copies licensed, but otherwise for archival purposes only.

2.4 Benchmarking. You may use the Software to conduct internal performance testing and benchmarking studies. You may only publish or otherwise distribute the results of such studies to third parties as follows: (a) if with respect to VMware's Workstation or Fusion products, only if You provide a copy of Your study to benchmark@vmware.com prior to distribution; (b) if with respect to any other Software, only if VMware has reviewed and approved of the methodology, assumptions and other parameters of the study (please contact VMware at benchmark@vmware.com to request such review and approval) prior to such publication and distribution.

2.5 VMware Tools. You may distribute the VMware Tools to third parties solely when installed in a Guest Operating System within a Virtual Machine. You are liable for compliance by those third parties with the terms and conditions of this EULA.

2.6 Open Source Software. Notwithstanding anything herein to the contrary, Open Source Software is licensed to You under such OSS's own applicable license terms, which can be found in the open_source_licenses.txt file, the Documentation or as applicable, the corresponding source files for the Software available at www.vmware.com/download/open_source.html. These OSS license terms are consistent with the license granted in Section 2 (License Grant), and may contain additional rights benefiting You. The OSS license terms shall take precedence over this EULA to the extent that this EULA imposes greater restrictions on You than the applicable OSS license terms. To the extent the license for any Open Source Software requires VMware to make available to You the corresponding source code and/or modifications (the "Source Files"), You may obtain a copy of the applicable Source Files from VMware's website at www.vmware.com/download/open_source.html or by sending a written request, with Your name and address to: VMware, Inc., 3401 Hillview Avenue, Palo Alto, CA 94304, United States of America. All requests should clearly specify: Open Source Files Request, Attention: General Counsel. This offer to obtain a copy of the Source Files is valid for three years from the date You acquired this Software.

3. RESTRICTIONS; OWNERSHIP.

3.1 License Restrictions. Without VMware's prior written consent, You must not, and must not allow any third party to: (a) use Software in an application services provider, service bureau, or similar capacity for third parties, except that You may use the Software to deliver hosted services to Your Affiliates; (b) disclose to any third party the results of any benchmarking testing or comparative or competitive analyses of VMware's Software done by or on behalf of You, except as specified in Section 2.4 (Benchmarking); (c) make available Software in any form to anyone other than Your employees or contractors reasonably acceptable to VMware and require access to use Software on behalf of You in a matter permitted by this EULA, except as specified in Section 2.2 (Third Party Agents); (d) transfer or sublicense Software or Documentation to an Affiliate or any third party, except as expressly permitted in Section 12.1 (Transfers; Assignment); (e) use Software in conflict with the terms and restrictions of the Software's licensing model and other requirements specified in Product Guide and/or VMware quote; (f) except to the extent permitted by applicable mandatory law, modify, translate, enhance, or create derivative works from the Software, or reverse engineer, decompile, or otherwise attempt to derive source code from the Software, except as specified in Section 3.2 (Decompilation); (g) remove any copyright or other proprietary notices on or in any copies of Software; or (h) violate or circumvent any technological restrictions within the Software or specified in this EULA, such as via software or services.

3.2 Decompilation. Notwithstanding the foregoing, decompiling the Software is permitted to the extent the laws of the Territory give You the express right to do so to obtain information necessary to render the Software interoperable with other software; provided, however, You must first request such information from VMware, provide all reasonably requested information to allow VMware to assess Your claim, and VMware may, in its discretion, either provide such interoperability information to You, impose reasonable conditions, including a reasonable fee, on such use of the Software, or offer to provide alternatives to ensure that VMware's proprietary rights in the Software are protected and to reduce any adverse impact on VMware's proprietary rights.

3.3 Ownership. The Software and Documentation, all copies and portions thereof, and all improvements, enhancements, modifications and derivative works thereof, and all Intellectual Property Rights therein, are and shall remain the sole and exclusive property of VMware and its licensors. Your rights to use the Software and Documentation shall be limited to those expressly granted in this EULA and any applicable Order. No other rights with respect to the Software or any related Intellectual Property Rights are implied. You are not authorized to use (and shall not permit any third party to use) the Software, Documentation or any portion thereof except as expressly authorized by this EULA or the applicable Order. VMware reserves all rights not expressly granted to You. VMware does not transfer any ownership rights in any Software.

3.4 Guest Operating Systems. Certain Software allows Guest Operating Systems and application programs to run on a computer system. You acknowledge that You are responsible for obtaining and complying with any licenses necessary to operate any such third-party software.

4. ORDER. Your Order is subject to this EULA. No Orders are binding on VMware until accepted by VMware. Orders for Software are deemed to be accepted upon VMware's delivery of the Software included in such Order. Orders issued to VMware do not have to be signed to be valid and enforceable.

5. RECORDS AND AUDIT. During the License Term for Software and for two (2) years after its expiration or termination, You will maintain accurate records of Your use of the Software sufficient to show compliance with the terms of this EULA. During this period, VMware will have the right to audit Your use of the Software to confirm compliance with the terms of this EULA. That audit is subject to reasonable notice by VMware and will not unreasonably interfere with Your business activities. VMware may conduct no more than one (1) audit in any twelve (12) month period, and only during normal business hours. You will reasonably cooperate with VMware and any third party auditor and will, without prejudice to other rights of VMware, address any non-compliance identified by the audit by promptly paying additional fees. You will promptly reimburse VMware for all reasonable costs of the audit if the audit reveals either underpayment of more than five (5%) percent of the Software fees payable by You for the period audited, or that You have materially failed to maintain accurate records of Software use.

6. SUPPORT AND SUBSCRIPTION SERVICES. Except as expressly specified in the Product Guide, VMware does not provide any support or subscription services for the Software under this EULA. You have no rights to any updates, upgrades or extensions or enhancements to the Software developed by VMware unless you separately purchase VMware support or subscription services. These support or subscription services are subject to the Support Services Terms.

7. WARRANTIES.

7.1 Software Warranty, Duration and Remedy. VMware warrants to You that the Software will, for a period of ninety (90) days following notice of availability for electronic download or delivery ("Warranty Period"), substantially conform to the applicable Documentation, provided that the Software: (a) has been properly installed and used at all times in accordance with the applicable Documentation; and (b) has not been modified or added to by persons other than VMware or its authorized representative. VMware will, at its own expense and as its sole obligation and Your exclusive remedy for any breach of this warranty, either replace that Software or correct any reproducible error in that Software reported to VMware by You in writing during the Warranty Period. If VMware determines that it is unable to correct the error or replace the Software, VMware will refund to You the amount paid by You for that Software, in which case the License for that Software will terminate.

7.2 Software Disclaimer of Warranty. OTHER THAN THE WARRANTY ABOVE, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VMWARE AND ITS SUPPLIERS MAKE NO OTHER EXPRESS WARRANTIES UNDER THIS EULA, AND DISCLAIM ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ANY WARRANTY ARISING BY STATUTE, OPERATION OF LAW, COURSE OF DEALING OR PERFORMANCE, OR USAGE OF TRADE. VMWARE AND ITS LICENSORS DO NOT WARRANT THAT THE SOFTWARE WILL OPERATE UNINTERRUPTED OR THAT IT WILL BE FREE FROM DEFECTS OR THAT IT WILL MEET YOUR REQUIREMENTS.

8. INTELLECTUAL PROPERTY INDEMNIFICATION.

8.1 Defense and Indemnification. Subject to the remainder of this Section 8 (Intellectual Property Indemnification), VMware shall defend You against any third party claim that the Software infringes any patent, trademark or copyright of such third party, or misappropriates a trade secret (but only to the extent that the misappropriation is not a result of Your actions) under the laws of: (a) the United States and Canada; (b) the European Economic Area; (c) Australia; (d) New Zealand; (e) Japan; or (f) the People's Republic of China, to

the extent that such countries are part of the Territory for the License ("Infringement Claim") and indemnify You from the resulting costs and damages finally awarded against You to such third party by a court of competent jurisdiction or agreed to in settlement. The foregoing obligations are applicable only if You: (i) promptly notify VMware in writing of the Infringement Claim; (ii) allow VMware sole control over the defense for the claim and any settlement negotiations; and (iii) reasonably cooperate in response to VMware requests for assistance. You may not settle or compromise any Infringement Claim without the prior written consent of VMware.

8.2 Remedies. If the alleged infringing Software become, or in VMware's opinion be likely to become, the subject of an Infringement Claim, VMware will, at VMware's option and expense, do one of the following: (a) procure the rights necessary for You to make continued use of the affected Software; (b) replace or modify the affected Software to make it non-infringing; or (c) terminate the License to the affected Software and discontinue the related support services, and, upon Your certified deletion of the affected Software, refund: (i) the fees paid by You for the License to the affected Software, less straight-line depreciation over a three (3) year useful life beginning on the date such Software was delivered; and (ii) any pre-paid service fee attributable to related support services to be delivered after the date such service is stopped. Nothing in this Section 8.2 (Remedies) shall limit VMware's obligation under Section 8.1 (Defense and Indemnification) to defend and indemnify You, provided that You replace the allegedly infringing Software upon VMware's making alternate Software available to You and/or You discontinue using the allegedly infringing Software upon receiving VMware's notice terminating the affected License.

8.3 Exclusions. Notwithstanding the foregoing, VMware will have no obligation under this Section 8 (Intellectual Property Indemnification) or otherwise with respect to any claim based on: (a) a combination of Software with non-VMware products (other than non-VMware products that are listed on the Order and used in an unmodified form); (b) use for a purpose or in a manner for which the Software was not designed; (c) use of any older version of the Software when use of a newer VMware version would have avoided the infringement; (d) any modification to the Software made without VMware's express written approval; (e) any claim that relates to open source software or freeware technology or any derivatives or other adaptations thereof that is not embedded by VMware into Software listed on VMware's commercial price list; or (f) any Software provided on a no charge, beta or evaluation basis. THIS SECTION 8 (INTELLECTUAL PROPERTY INDEMNIFICATION) STATES YOUR SOLE AND EXCLUSIVE REMEDY AND VMWARE'S ENTIRE LIABILITY FOR ANY INFRINGEMENT CLAIMS OR ACTIONS.

9. LIMITATION OF LIABILITY.

9.1 Limitation of Liability. TO THE MAXIMUM EXTENT MANDATED BY LAW, IN NO EVENT WILL VMWARE AND ITS LICENSORS BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE, LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY, OR OTHERWISE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE PRECEDING LIMITATION MAY NOT APPLY TO YOU. VMWARE'S AND ITS LICENSORS' LIABILITY UNDER THIS EULA WILL NOT, IN ANY EVENT, REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE, EXCEED THE GREATER OF THE LICENSE FEES YOU PAID FOR THE SOFTWARE GIVING RISE TO THE CLAIM OR $5000. THE FOREGOING LIMITATIONS SHALL APPLY REGARDLESS OF WHETHER VMWARE OR ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

9.2 Further Limitations. VMware's licensors shall have no liability of any kind under this EULA and VMware's liability with respect to any third party software embedded in the Software shall be subject to Section 9.1 (Limitation of Liability). You may not bring a claim under this EULA more than eighteen (18) months after the cause of action arises.

10. TERMINATION.

10.1 EULA Term. The term of this EULA begins on the notice of availability for electronic download or delivery of the Software and continues until this EULA is terminated in accordance with this Section 10.

10.2 Termination for Breach. VMware may terminate this EULA effective immediately upon written notice to You if: (a) You fail to pay any portion of the fees under an applicable Order within ten (10) days after receiving written notice from VMware that payment is past due; or (b) You breach any other provision of this EULA and fail to cure within thirty (30) days after receipt of VMware's written notice thereof.

10.3 Termination for Insolvency. VMware may terminate this EULA effective immediately upon written notice to You if You: (a) terminate or suspend your business; (b) become insolvent, admit in writing Your inability to pay Your debts as they mature, make an assignment for the benefit of creditors; or become subject to control of a trustee, receiver or similar authority; or (c) become subject to any bankruptcy or insolvency proceeding.

10.4 Effect of Termination. Upon VMware's termination of this EULA: (a) all Licensed rights to all Software granted to You under this EULA will immediately cease; and (b) You must cease all use of all Software, and return or certify destruction of all Software and License Keys (including copies) to VMware, and return, or if requested by VMware, destroy, any related VMware Confidential Information in Your possession or control and certify in writing to VMware that You have fully complied with these requirements. Any provision will survive any termination or expiration if by its nature and context it is intended to survive, including Sections 1 (Definitions), 2.6 (Open Source Software), 3 (Restrictions; Ownership), 5 (Records and Audit), 7.2 (Software Disclaimer of Warranty), 9 (Limitation of Liability), 10 (Termination), 11 (Confidential Information) and 12 (General).

11. CONFIDENTIAL INFORMATION.

11.1 Definition. "Confidential Information" means information or materials provided by one party (" **Discloser**") to the other party ("Recipient") which are in tangible form and labelled "confidential" or the like, or, information which a reasonable person knew or should have known to be confidential. The following information shall be considered Confidential Information whether or not marked or identified as such: (a) License Keys; (b) information regarding VMware's pricing, product roadmaps or strategic marketing plans; and (c) non-public materials relating to the Software.

11.2 Protection. Recipient may use Confidential Information of Discloser; (a) to exercise its rights and perform its obligations under this EULA; or (b) in connection with the parties' ongoing business relationship. Recipient will not use any Confidential Information of Discloser for any purpose not expressly permitted by this EULA, and will disclose the Confidential Information of Discloser only to the employees or contractors of Recipient who have a need to know such Confidential Information for purposes of this EULA and who are under a duty of confidentiality no less restrictive than Recipient's duty hereunder. Recipient will protect Confidential Information from unauthorized use, access, or disclosure in the same manner as Recipient protects its own confidential or proprietary information of a similar nature but with no less than reasonable care.

11.3 Exceptions. Recipient's obligations under Section 11.2 (Protection) with respect to any Confidential Information will terminate if Recipient can show by written records that such information: (a) was already known to Recipient at the time of disclosure by Discloser; (b) was disclosed to Recipient by a third party who had the right to make such disclosure without any confidentiality restrictions; (c) is, or through no fault of Recipient has become, generally available to the public; or (d) was independently developed by Recipient without access to, or use of, Discloser's Information. In addition, Recipient will be allowed to disclose Confidential Information to the extent that such disclosure is required by law or by the order of a court of similar judicial or administrative body, provided that Recipient notifies Discloser of such required disclosure promptly and in writing and cooperates with Discloser, at Discloser's request and expense, in any lawful action to contest

or limit the scope of such required disclosure.

11.4 Data Privacy. You agree that VMware may process technical and related information about Your use of the Software which may include internet protocol address, hardware identification, operating system, application software, peripheral hardware, and non-personally identifiable Software usage statistics to facilitate the provisioning of updates, support, invoicing or online services and may transfer such information to other companies in the VMware worldwide group of companies from time to time. To the extent that this information constitutes personal data, VMware shall be the controller of such personal data. To the extent that it acts as a controller, each party shall comply at all times with its obligations under applicable data protection legislation.

12. GENERAL.

12.1 Transfers; Assignment. Except to the extent transfer may not legally be restricted or as permitted by VMware's transfer and assignment policies, in all cases following the process set forth at www.vmware.com/support/policies/licensingpolicies.html, You will not assign this EULA, any Order, or any right or obligation herein or delegate any performance without VMware's prior written consent, which consent will not be unreasonably withheld. Any other attempted assignment or transfer by You will be void. VMware may use its Affiliates or other sufficiently qualified subcontractors to provide services to You, provided that VMware remains responsible to You for the performance of the services.

12.2 Notices. Any notice delivered by VMware to You under this EULA will be delivered via mail, email or fax.

12.3 Waiver. Failure to enforce a provision of this EULA will not constitute a waiver.

12.4 Severability. If any part of this EULA is held unenforceable, the validity of all remaining parts will not be affected.

12.5 Compliance with Laws; Export Control; Government Regulations. Each party shall comply with all laws applicable to the actions contemplated by this EULA. You acknowledge that the Software is of United States origin, is provided subject to the U.S. Export Administration Regulations, may be subject to the export control laws of the applicable territory, and that diversion contrary to applicable export control laws is prohibited. You represent that (1) you are not, and are not acting on behalf of, (a) any person who is a citizen, national, or resident of, or who is controlled by the government of any country to which the United States has prohibited export transactions; or (b) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List; and (2) you will not permit the Software to be used for, any purposes prohibited by law, including, any prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons. The Software and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation", respectively, pursuant to DFARS Section 227.7202 and FAR Section 12.212(b), as applicable. Any use, modification, reproduction, release, performing, displaying or disclosing of the Software and documentation by or for the U.S. Government shall be governed solely by the terms and conditions of this EULA.

12.6 Construction. The headings of sections of this EULA are for convenience and are not to be used in interpreting this EULA. As used in this EULA, the word 'including' means "including but not limited to".

12.7 Governing Law. This EULA is governed by the laws of the State of California, United States of America (excluding its conflict of law rules), and the federal laws of the United States. To the extent permitted by law, the state and federal courts located in Santa Clara County, California will be the exclusive jurisdiction for disputes arising out of or in connection with this EULA. The U.N. Convention on Contracts for the International Sale of Goods does not apply.

12.8 Third Party Rights. Other than as expressly set out in this EULA, this EULA does not create any rights for any person who is not a party to it, and no person who is not a party to this EULA may enforce any of its

terms or rely on any exclusion or limitation contained in it.

12.9 Order of Precedence. In the event of conflict or inconsistency among the Product Guide, this EULA and the Order, the following order of precedence shall apply: (a) the Product Guide, (b) this EULA and (c) the Order. With respect to any inconsistency between this EULA and an Order, the terms of this EULA shall supersede and control over any conflicting or additional terms and conditions of any Order, acknowledgement or confirmation or other document issued by You.

12.10 Entire Agreement. This EULA, including accepted Orders and any amendments hereto, and the Product Guide contain the entire agreement of the parties with respect to the subject matter of this EULA and supersede all previous or contemporaneous communications, representations, proposals, commitments, understandings and agreements, whether written or oral, between the parties regarding the subject matter hereof. This EULA may be amended only in writing signed by authorized representatives of both parties.

12.11 Contact Information. Please direct legal notices or other correspondence to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America, Attention: Legal Department.

vmware®

VMware, Inc. Support and Subscription Services "SnS" Terms and Conditions

VMware, Inc., a Delaware corporation, or VMware International Limited, a company organized under the laws of Ireland, as applicable (**"VMware"**), shall provide Technical Support and Subscription Services (as defined herein) (collectively, the **"Services")** to the Customer, per the terms of this Agreement (the "**Agreement**") and as set forth at the VMware Support Services Website, at http://www.vmware.com/support/services/. The applicable VMware entity, **Effective Date**, **Software**, and Services level will be set forth on the applicable enterprise license agreement, SnS order form, Customer's purchase Order, or, if Customer has purchased support on a per-incident basis (**"Per Incident"**), in the registration form completed by Customer upon such purchase (collectively the **"Order"**).

1. Definitions.

1.1 "**Error**" means a failure in the Software to materially conform to the specifications described in the applicable product documentation ("**Documentation**").

1.2 "**Modified Code**" means any modification, addition and/or development of code scripts deviating from the predefined product code tree(s)/modules developed by VMware for production deployment or use. Modified Code excludes customizable Software options for which VMware offers Services on the applicable VMware price list.

1.3 "**Services Fees**" means the fees for Services specified in a corresponding VMware or reseller invoice.

1.4 "**Services Period**" means the period for which Customer has purchased the Services and any subsequent renewal periods and shall commence: (a) for Software licenses for which Services are mandatory, on the date the applicable Software license key(s) are made available for download, and (b) for Software licenses for which Services are optional, on the date of purchase of the Services.

1.5 "**Severity**" is a measure of the relative impact an Error has on the use of the Software, as determined by VMware. The following Severity levels apply to all Software:

(a) "**Severity One**" means Customer's production server or other mission critical system(s) are down and no workaround is immediately available and (i) all or a substantial portion of Customer's mission critical data is at a significant risk of loss or corruption; (ii) Customer has had a substantial loss of service; or (iii) Customer's business operations have been severely disrupted.

(b) "**Severity Two**" means that major functionality is severely impaired such that (i) operations can continue in a restricted fashion, although long-term productivity might be adversely affected; (ii) a major milestone is at risk; ongoing and incremental installations are affected; or (iii) a temporary workaround is available.

(c) "**Severity Three**" means a partial, non-critical loss of functionality of the software such that: (i) the operation of some component(s) is impaired but allows the user to continue using the Software; or (ii) initial installation milestones are at minimal risk.

(d) "**Severity Four**" means (i) general usage questions and cosmetic issues, including errors in the documentation, and (ii) cases opened via email for Zimbra Software.

1.6 "**Software**" means software offered on the VMware price list, and all components shipped with the Software, including Open Source components.

1.7 "**Subscription Services**" means any Maintenance Releases, Minor Releases and Major Releases (each defined below) to the Software, and their Documentation, that VMware provides to Customer.

(a) "**Maintenance Release**" or "**Update**" means a generally available release of the Software that typically provides maintenance corrections or fixes only, designated by VMware by means of a change in the digit to the right of the second decimal point (e.g. Software 5.0 >> Software 5.0.1), or for certain Software, by means of a change in the digit of the Update number (e.g. Software 5.0 Update 1).

(b) "**Minor Release**" means a generally available release of the Software that (i) introduces a limited amount of new features and functionality, and (ii) is designated by VMware by means of a change in the digit to the right of the decimal point (e.g., Software 5.0>>Software 5.1).

(c) "**Major Release,**" also known as an "**Upgrade,**" means a generally available release of the Software that (i) contains functional enhancements or extensions, and (ii) is designated by VMware by means of a change in the digit to the left of the first decimal point (e.g., Software 5.0 >> Software 6.0).

1.8 "**Technical Support**" means the provision of telephone or web-based technical assistance by VMware to Customer's technical contact(s) with respect to installation and Errors, at the corresponding Services level purchased by Customer.

1.9 "**Third Party Products**" means any software or hardware that (i) is manufactured by a party other than VMware and (ii) has not been incorporated into the Software.

vmware®

2. Service Terms.

2.1 Provision of Services. Subject to the terms of this Agreement, VMware shall provide Services to Customer during the Services Period at the Services level purchased. Customer's use of a Subscription Services release will be subject to the terms of the VMware Product Guide posted at www.vmware.com/download/eula on the date Customer first installs that release.

2.2 End of Availability. VMware may, at its discretion, decide to retire Software and/or Services from time to time ("**End of Availability**"). VMware shall post notice of End of Availability, including the last date of general commercial availability of the affected Software and the timeline for discontinuing Services, at https://www.vmware.com/support/policies/lifecycle.html. VMware shall have no obligation to provide Services for Software that is outside of the applicable Service life.

2.3 Purchase Requirements.

(a) Except as otherwise provided for by VMware, Customer may purchase initial Services only for the most current, generally available release of the Software.

(b) Customer must purchase and/or renew Services at the same Services level for all of the Software in a given environment (e.g., Test, Development, QA, Production).

(c) Except as otherwise provided in the applicable price list, the minimum term for any Service offering is one (1) year.

(d) These Services terms and conditions will automatically update to VMware's then-current Services terms and conditions set forth at https://www.vmware.com/files/pdf/support/support_terms_conditions.pdf upon any renewal of Services.

2.4 Exclusions.

(a) Services do not cover problems caused by the following:

(i) accident; unusual physical, electrical or electromagnetic stress; neglect; misuse; failure of electric power, air conditioning or humidity control; failure of rotation media not furnished by VMware; operation of the Software with other media not in accordance with the manufacturer's specifications; or causes other than ordinary use;

(ii) improper installation by Customer or use of the Software that deviates from any operating procedures as specified in the Documentation;

(iii) Third Party Products, other than the interface of the Software with the Third Party Products;

(iv) Modified Code;

(v) issues relating to Software offered as a Service ("SaaS");

(vi) any customized deliverables created by VMware specifically for Customer as part of consulting services; or(viii); use of the Software with unsupported tools (i.e., Java Development Kit (JDK); Java Runtime Environment (JRE)), APIs, interfaces or data formats other than those included with the Software and supported as set forth in the Documentation; or

(vii) any issue not covered by Technical Support.

Customer may request assistance from VMware for such problems, for an additional fee.

(b) In the event that VMware suspects that a reported problem may be related to Modified Code, VMware, may, in its sole discretion, (i) request that the Modified Code be removed, and/or (ii) inform Customer that additional assistance may be obtained by Customer directly from various product discussion forums or by engaging VMware's consulting services group for an additional fee.

2.5 Customer Responsibilities. VMware's obligations regarding Services are subject to the following:

(a) Customer agrees to receive from VMware communications via e-mail, telephone, and other formats, regarding Services (such as communications concerning support coverage, Errors or other technical issues and the availability of new releases of the Software).

(b) Customer's technical contact shall cooperate to enable VMware to deliver the Services.

(c) Customer is solely responsible for the use of the Software by its personnel and shall properly train its personnel in the use and application of the Software.

(d) Customer shall promptly report to VMware all problems with the Software, and shall implement any corrective procedures provided by VMware reasonably promptly after receipt.

(e) Customer is solely responsible for protecting and backing up the data and information stored on the computers on which the Software is used and should confirm that such data and information is protected and backed up in accordance with any internal or regulatory

requirements as applicable, before contacting VMware for Technical Support. VMware is not responsible for lost data or information in the event of errors or other malfunction of the Software or computers on which the Software is used.

(f) Customer will have dedicated resources available to work 24X7 on Severity One Errors.

3. Services Offerings and Fees.

3.1 Services Fee Terms.

(a) Services Fees are payable on the Effective Date or, in the case of a renewal term, no later than the date of commencement of the applicable Services Period. Services Fees are specified in the applicable price list and are non-refundable.

(b) In the event that Customer renews or adds a Services offering that has a minimum term of one (1) year, Customer may elect to make Services for all or a portion of its Software licenses coterminous with the renewed or added Services. In such case, VMware will prorate the applicable Services Fees to extend the current Services Period to make it coterminous with such renewed or added Services.

(c) For Software that is licensed on a perpetual basis, if a Customer purchases Services after acquiring the Software licenses, or had elected not to renew Services and later wishes to re-enroll in the Services, Customer must move to the then-current Major Release of the Software and must pay: (i) the applicable Services Fees for the current Services Period; (ii) the amount of Services Fees that would have been paid for the period of time that Customer had not enrolled in the Services, and (iii) a twenty-percent (20%) reinstatement fee on the sum of the Services Fees in (i) and (ii).

(d) In cases where Customer purchases a License to migrate up from one edition of the Software to another (e.g., VMware vSphere Standard to VMware vSphere Enterprise Plus), any unused period of the Services Period on the original License will be converted and used to extend the Services Period for the newly purchased upgraded License. This paragraph (d) shall not apply to enterprise license agreements.

(e) If Customer originally purchased Services from a VMware Authorized Service Provider and is now renewing only Technical Support through such VMware Authorized Service Provider, Customer may purchase Subscription Services separately on a renewal basis from VMware. The renewal fee for such Subscription Services shall be as set forth in the applicable price list. "**Authorized Service Provider**" means a third party that is authorized under contract by VMware to provide first and/or second level Technical Support for the Software.

3.2 Advanced and Complimentary Offerings.

(a) Certain Services (e.g., Business Critical Support and Mission Critical Support) require that Customer also purchase a base level of support. See the applicable price list for details.

(b) VMware may offer complimentary Services, including VMware Complimentary Update Services for certain Software, as more fully described at the VMware Technical Support Services website. "**VMware Complimentary Update Services**" means any Maintenance Releases and Minor Releases that VMware provides to Customer. This VMware Complimentary Update Service does not include any Major Releases.

4. Miscellaneous Terms

4.1 Payment Terms. Services Fees are exclusive of any taxes, duties, or similar charges imposed by any government. Customer shall pay or reimburse VMware for all federal, state, dominion, provincial, or local sales, use, personal property, excise, value added, withholding or other taxes, fees, or duties relating to the transactions contemplated by this Agreement (other than taxes on the net income of VMware). All invoices issued hereunder by VMware are due and payable within thirty (30) days of the date of the invoice. Amounts not paid on time are subject to a late charge equal to the lesser of one and one-half percent (1.5%) per month or the maximum amount allowed by applicable law. If payment of any Services Fee is overdue, VMware may also suspend performance until such delinquency is corrected.

4.2 Limited Warranty. VMware warrants that the Services to be performed hereunder will be done in a workmanlike manner and shall conform to industry standards. Upon Customer providing VMware with a reasonably detailed written notice to cure within thirty (30) days of occurrence of the nonconformance, VMware will re-perform the Services to achieve commercially reasonable conformance with the above warranty. TO THE MAXIMUM EXTENT PERMITTED BY LAW, THIS WARRANTY IS GIVEN EXPRESSLY AND IN PLACE OF ALL OTHER WARRANTIES, STATUTORY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. TO THE MAXIMUM EXTENT MANDATED BY LAW, THIS REMEDY WILL BE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO NONCONFORMANCE OF SERVICES.

4.3 Limitation of Liability. TO THE MAXIMUM EXTENT PERMITTED BY LAW, VMWARE SHALL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER BASED UPON CONTRACT, TORT OR ANY OTHER LEGAL THEORY, ARISING FROM ITS PERFORMANCE OR NON-PERFORMANCE UNDER THIS AGREEMENT. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE PRECEDING LIMITATION MAY NOT APPLY TO CUSTOMER. VMWARE'S LIABILITY UNDER THIS AGREEMENT WILL NOT, IN ANY EVENT, EXCEED THE SERVICES FEES PAID BY CUSTOMER TO VMWARE UNDER THIS AGREEMENT DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE DATE OF THE EVENT MOST DIRECTLY GIVING RISE TO THE CLAIM.

4.4 Termination. VMware may terminate the Agreement and all Services at any time if (1) it is discovered that Customer is currently in breach of its Software license restrictions, pursuant to Customer's Software license or (2) Customer is in material breach of this Agreement.

4.5 Data Protection. Customer acknowledges that correspondence and log files generated in conjunction with a request for Services may contain sensitive, confidential or personal information. Customer is solely responsible for taking the steps it considers necessary to protect such data, including obfuscating the logs or otherwise guarding such information prior to sending it to VMware.

4.6 Other. Customer may not assign or delegate this Agreement to any third party without the prior written consent of VMware. This Agreement shall be governed by the laws of the State of California without regard to conflict of laws principles. The parties consent to the exclusive jurisdiction of the state and federal courts located in Santa Clara County, California. This Agreement constitutes the entire agreement of the parties with respect to the provision of the Services by VMware to Customer, and supersedes all prior written or oral communications, understandings and agreements. This Agreement may not be amended except in a written document signed by both parties. Any waiver of the provisions of this Agreement must be in writing to be effective. Except as expressly set forth herein, no terms of any purchase order or other business form that Customer may use will affect the obligations of the parties under this Agreement, and any such purchase order or other business form of Customer which contains additional or conflicting terms are hereby rejected by VMware. Customer agrees that purchase orders do not have to be signed to be valid and enforceable. If any provision of this Agreement is found to be invalid or unenforceable, the remaining terms will continue to be valid and enforceable to the fullest extent permitted by law. The version of the Technical Support guide found at https://www.vmware.com/files/pdf/support/tech_support_guide.pdf and the policies located at https://www.vmware.com/support/policies/index/ are the governing versions of such documents/policies; any translation into other languages is for convenience only. VMware may update the Technical Support guide and support policies periodically, without prior notice.

Attachment B – Scope of Services Awarded to Contractor
Identification of Service Models Matrix

Offerors must complete the following form to identify the service models your firm offers under this RFP. You may provide a list of the different SaaS, IaaS, and/or PaaS services that you offer, including the Categorization of Risk that you have the ability to store and secure. This document is to provide purchasing entities and eligible users a quick snap shot of the cloud solutions your firm provides.

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
SaaS				
Mobile Device Management				
VMware AirWatch Mobile Device Management	✓			Public, Private
Container Management				
VMware AirWatch Container Management	✓			Public, Private
Mobile Application Management				
VMware AirWatch Application Management	✓			Public, Private
Mobile Content Management				
VMware AirWatch Content Management	✓			Public, Private
Mobile Email Management				
VMware AirWatch Content Management	✓			Public, Private

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
Mobile Browsing Management				
VMware AirWatch Browsing Management	✓			Public, Private
Telecom Management				
VMware AirWatch Telecom Management	✓			Public, Private
Laptop Management				
VMware AirWatch Laptop Management	✓			Public, Private
Rugged Device Management				
VMware AirWatch Rugged Device Management	✓			Public, Private
Multiuser Management				
VMware AirWatch Multiuser Management	✓			Public, Private
Collaboration				
AirWatch Content Locker	✓			Public, Private
Video Management				
AirWatch Video	✓			Public, Private
Secure Enterprise Social Networking				
Socialcast	✓			Public, Private

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
Identity Management				
VMware Identity Manager	✓			Public, Private
Compliance				
VMware vRealize Air Compliance	✓			Public
IaaS				
On Demand Infrastructure as a Service				
VMware vCloud Air Virtual Private Cloud OnDemand	✓			Public, Hybrid, Community
Dedicated Infrastructure as a Service				
VMware vCloud Air Dedicated Cloud	✓			Public, Hybrid, Community
Virtual Private Infrastructure as a Service				
VMware vCloud Air Virtual Private Cloud	✓			Public, Hybrid, Community
Business Continuity/Disaster Recovery				
VMware vCloud Air Disaster Recovery	✓			Public, Hybrid, Community
Data Protection				
VMware vCloud Air Data Protection	✓			Public, Hybrid, Community
Data Replication				

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
VMware Continuent	✓			Public, Hybrid, Community
Storage: Block Storage				
VMware vCloud Air Block Storage	✓			Public, Hybrid, Community
Storage: Object Storage				
VMware vCloud Air Object Storage	✓			Public, Hybrid, Community
Networking				
VMware vCloud Air Networking	✓			Public, Hybrid, Community
Advanced Networking Services				
VMware vCloud Air Advanced Networking Services	✓			Public, Hybrid, Community
Networking: Direct Link				
VMware vCloud Air Direct Connect	✓			Public, Hybrid, Community
Networking: Hybrid Networking				
VMware vCloud Air Hybrid Cloud Manager	✓			Public, Hybrid, Community
PC/Desktop "aaS"				
VMware Horizon Air Desktops and Apps	✓			Public, Hybrid, Community
Private, Hybrid, and Community IaaS Enablement				

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
IaaS Suite				
VMware vCloud Suite	✓			Private, Hybrid, Community
Cloud Management Platform				
VMware vRealize Suite	✓			Private, Hybrid, Community
Cloud Automation				
VMware vRealize Automation	✓			Private, Hybrid, Community
Cloud Operations Management				
VMware vRealize Operations	✓			Private, Hybrid, Community
Cloud Log Management				
VMware vRealize Log Insight	✓			Private, Hybrid, Community
Cloud Business Management				
VMware vRealize Business	✓			Private, Hybrid, Community
Software Defined Networking				
VMware NSX	✓			Private, Hybrid, Community
Software Defined Storage				
VMware Virtual SAN	✓			Private, Hybrid, Community

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
Hybrid Cloud Management Enablement				
vRealize Operations and Automation Public Cloud Extensions (available as add-ons to vCloud Suite)	✓			Private, Hybrid, Community
Virtualization Infrastructure				
VMware vSphere	✓			Private, Hybrid, Community
Virtual Desktop Infrastructure				
VMware Horizon	✓			Private, Hybrid
PaaS				
N/A				

Attachment C – Cost Schedule
(VMware, Inc.)

Solicitation Number CH16012
NASPO ValuePoint Cloud Solutions RFP

Cloud Solutions By Category. Specify ***Discount Percent %*** Offered for products in each category. Highest discount will apply for products referenced in detail listings for multiple categories. Provide a detailed product offering for each category.

Software as a Service	**Discount % 2.27% ****
(1) AirWatch Mobile Device Management	
(2) vRealize Air Compliance	
(3) SocialCast	
Infrastructure as a Service	**Discount % 7.00% ****
(1) VMware vCloud Air	
(2) OnDemand Cloud	
Platform as a Services	**Discount % Not Offering**
Value Added Services	**Discount % See Below**
(1) IaaS Private, Hybrid, & Community Cloud Enablement	**Discount %: 4.00% ****
(2) IaaS Private, Hybrid, & Community Cloud Enablement Support	**Discount %: 2.00% ****

** The minimum discounts provided are in-line with the minimum discounts offered under VMware's Federal GSA Schedule 70 and other similar contracts (i.e. no commitment contracts or procurement vehicles) that VMware is currently negotiating.

VMware will hold the discounts listed above constant for the term of the contract. These discounts reflect the minimum discount that customers will receive when placing an order. If VMware (or an authorized reseller) fulfills an order under the contract, they may offer the customer greater discounts than the contract minimum discounts provided. Discounts for orders may vary by transaction, but will always be at least at the minimum discount listed above.

In addition, VMware will pay NASPO ValuePoint their administrative fee of 0.25%. If another participating entity executes a Participating Addendum with VMware and they require a subsequent administrative fee, VMware will pay that entity the agreed upon administrative fee.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal
March 10, 2016

Additional Value Added Services:

Maintenance Services

+ **Onsite Hourly Rate $210.00 - $532.00**
+ **Remote Hourly Rate $155.00 - $477.00**

Professional Services

- **Deployment Services**
  + **Onsite Hourly Rate $210.00 - $532.00**
  + **Remote Hourly Rate $155.00 - $477.00**
- **Consulting/Advisory Services**
  + **Onsite Hourly Rate $210.00 - $532.00**
  + **Remote Hourly Rate $155.00 - $477.00**
- **Architectural Design Services**
  + **Onsite Hourly Rate $210.00 - $532.00**
  + **Remote Hourly Rate $155.00 - $477.00**
- **Statement of Work Services**
  + **Onsite Hourly Rate $210.00 - $532.00**
  + **Remote Hourly Rate $155.00 - $477.00**

+ Provided in the table below are the VMware Not to Exceed (NTE) Rates that will be used for Maintenance and Professional Services. The NTE Rates provided (both Remote and Onsite) are only available for purchase in the following manner: (i) through an agreed upon Statement of Work (SOW) between the customer and VMware that identifies the specific deliverables at a fixed price for the deliverables and ii) if purchased as a block, a minimum of 40 hours must be purchased and consumed in a continuous 40 hour period. Based on the customer requirements, VMware will determine the appropriate VMware role(s) needed to satisfy the requirements of the SOW.

VMware Role	Not to Exceed Hourly Rate (Remote) +	Not to Exceed Hourly Rate (Onsite) +
Associate	$ 155.00	$ 210.00
Inside Project Manager	$ 180.00	$ 235.00
Consultant	$ 236.25	$ 291.25
Project Manager	$ 236.25	$ 291.25
Sr. Project Manager	$ 262.50	$ 317.50
Business Consultant	$ 271.00	$ 326.00
Program Manager	$ 281.25	$ 336.25
Sr. Consultant	$ 295.00	$ 350.00
Business Senior Consultant	$ 318.00	$ 373.00
Architect	$ 322.00	$ 377.00
Business Architect	$ 373.00	$ 428.00
Senior Architect	$ 393.75	$ 448.75
Enterprise Architect	$ 420.00	$ 475.00
Business Strategist	$ 454.00	$ 509.00

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal
March 10, 2016

Business Practice Principal	$ 477.00	$ 532.00

As discussed in the Q&A period, the State will allow for annual increase to the vendor's proposed hourly rates. To adjust for annual cost increases in labor, overhead, and other expenses, VMware is proposing that its NTE Rates be increased by 3.00% annually for each year of the contract term. The annual increase will take effect on the anniversary of the contract award date.

Payment Options

VMware is pleased to offer flexible payment options under the resulting contract. VMware will offer customized payments to qualified customers through a Payment Plan Agreement. In accordance with the each customer's requirements for annual payment or financing, the terms and conditions of the payment arrangement with VMware Financial Solutions ("VFS"), or its designated and/or approved funding partner, will be set forth between the purchaser and VFS its designated and/or approved VMware Funding partner. Please refer to **Appendix G** for a copy of the proposed financing document.

Partner Services

+ + Onsite Hourly Rate $150.00 - $295.00
+ + Remote Hourly Rate $95.00 - $240.00

+ +Provided in the table below are the Partner Services Not to Exceed (NTE) Rates that will be used for professional services provided by our resellers / partners. Each partner may agree to offer the rates: (i) through an agreed upon Statement of Work (SOW) between the customer and partner that identifies the specific deliverables at a fixed price for the deliverables, ii) or be purchased as a block of time.

Partner Rate Card	Not to Exceed Hourly Rate (Remote) + +	Not to Exceed Hourly Rate (Onsite) + +
Associate	$ 95.00	$ 150.00
Consultant	$ 135.00	$ 190.00
Managing Principal Consultant	$ 140.00	$ 195.00
Sr. Consultant	$ 190.00	$ 245.00
Consultant Architect	$ 170.00	$ 225.00
Sr. Architect	$ 220.00	$ 275.00
Enterprise Architect	$ 240.00	$ 295.00
Project / Engagement Manager	$ 135.00	$ 190.00

To adjust for annual cost increases in labor, VMware is proposing that its Partner NTE Rates be increased by 3.00% annually for each year of the contract term. The annual increase will take effect on the anniversary of the contract award date.

Training Deployment Services

+ + Onsite Hourly Rate $150.00 - $295.00
+ + Remote Hourly Rate $95.00 - $240.00

Please refer to the Partner Service Rates for any training requirements.

VMware, Inc. Response to:

NASPO ValuePoint Master Agreement for Cloud Solutions

State of Utah, Solicitation # CH16012

March 10, 2016

Submitted by: VMware, Inc. Mark Slafka, Capture Manager, US Public Sector, slafkam@vmware.com

This document is intended for Government consideration of VMware Inc.'s proposal offer and shall not be duplicated, used, or disclosed — in whole or in part — for any purpose other than to evaluate this document in accordance with the RFP CH16012 specifications. If a contract is awarded to VMware, Inc. as a result of, or in connection with the submission of this information, the Government shall have the right to duplicate, use, or disclose the information to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information obtained from another source without restriction. VMware Inc. agrees that the content of this proposal may be accessible to the public via Freedom of Information Act procedures or the state Open Records Law equivalent such as Utah's Government Records Access and Management Act (GRAMA).

Table of Contents

Compliance / Traceability Matrix 1

Section 1 Signature Page {5.1} 1

Cover Letter {5.2} 1

Acknowledgement of Amendments {5.3} 3

Section 2 Executive Summary {5.4} 4

Section 3 Mandatory Minimums {5.5} 7

3.1 GENERAL REQUIREMENTS {5.5} (M) 7

3.2 Recertification of Mandatory Minimums and Technical Specifications {5.7} 7

Section 4 Business Information {6} (M) (E) 8

4.1 Business Profile {6.1} (M) (E) 8

4.2 SCOPE OF EXPERIENCE {6.2} (M)(E) 11

4.3 FINANCIALS {6.3}(M) 12

4.4 GENERAL INFORMATION {6.4} (E) 14

4.5 BILLING AND PRICING PRACTICES{6.5}(E) 18

4.6 SCOPE AND VARIETY OF CLOUD SOLUTIONS {6.6}(E) 21

4.7 BEST PRACTICES {6.7} (E) 22

Section 5 Organization and Staffing {7} (ME) 25

5.1 Contract Manager {7.1} (ME) 25

Section 6 Technical Response {8} (ME) 27

6.1 TECHNICAL REQUIREMENTS {8.1} (M) (E) 27

6.1.2.1.a On-Demand Self-Service Capabilities of VMware's Public IaaS Services 28

6.1.2.1.b On-Demand Self Service Capabilities of VMware's Public SaaS Services 31

6.1.2.1.c On-Demand Self-Service Capabilities of VMware's Private, Hybrid, and Community IaaS Enablement Offerings 31

6.1.2.2.a Broad Network Access Capabilities of VMware's Public IaaS Services 32

6.1.2.2.b Broad Network Access Capabilities of VMware's Public SaaS Services 33

6.1.2.2.c Broad Network Access Capabilities of VMware's Private, Hybrid, and Community IaaS Enablement Offerings 33

6.1.2.3.a Resource Pooling Capabilities of VMware's Public IaaS Services 34

6.1.2.3.b Resource Pooling Capabilities of VMware's Public SaaS Services 34

6.1.2.3.c Resource Pooling Capabilities of VMware's Private, Hybrid, and Community IaaS Enablement Offerings 35

6.1.2.4.a Rapid Elasticity Capabilities of VMware's Public IaaS Services 36

6.1.2.4.b Rapid Elasticity Capabilities of VMware's Public SaaS Services 36

6.1.2.4.c Rapid Elasticity Capabilities of VMware's Private, Hybrid, and Community IaaS Enablement Offerings 37

6.1.2.5.a Measured Service Capabilities of VMware's Public IaaS Services 37

6.1.2.5.b Measured Service Capabilities of VMware's Public SaaS Services 38

6.1.2.5.c Measured Service Capabilities of VMware's Private, Hybrid, and Community IaaS Enablement Offerings 38

6.1.3.a VMware's Public Infrastructure as a Service (IaaS) Catalog 39
6.1.3.b VMware's Public SaaS Services Catalog 43
6.1.3.c VMware's Private, Hybrid and Community Cloud Catalog 46
6.1.4.a Affirmation of Willingness to Comply with the Requirements of Attachment C: NIST Service Models 52
6.1.4.b Affirmation of Willingness to Comply with the Requirements of Attachment D: Scope of Services 54
6.1.5 Adherence of VMware's Offerings to Services, Definitions, and Deployment models identified in RFP Attachment D 54
6.2 SUBCONTRACTORS {8.2} (E) 54
6.3 WORKING WITH PURCHASING ENTITIES –{8.3} (E) 57
6.3.1.a Data Breach Monitoring and Notification 58
6.3.1.b Personnel, Process, Timelines, and Methods of Communication and Assistance 58
6.3.1.c Prior to a Breach 58
6.3.1.d During and After a Breach 58
6.3.1.e Response time 59
6.4 CUSTOMER SERVICE {8.4} (E) 64
6.5 SECURITY OF INFORMATION {8.5} (E) 69
6.6 PRIVACY AND SECURITY {8.6} (E) 71
6.6.1 Compliance with NIST SP 800-145 and Other Relevant Standards 71
6.6.2 VMware's Government or Standards Organization Security Certifications 73
6.7 MIGRATION AND REDEPLOYMENT PLAN {8.7} (E) 84
6.8 SERVICE OR DATA RECOVERY {8.8} (E) 85
6.9 DATA PROTECTION {8.9}(E) 91
6.10 SERVICE LEVEL AGREEMENTS {8.10} (E) 93
6.11 DATA DISPOSAL {8.11} (E) 94
6.12 PERFORMANCE MEASURES AND REPORTING {8.12} (E) 94
6.13 CLOUD SECURITY ALLIANCE {8.13} (E) 100
6.14 SERVICE PROVISIONING {8.14} (E) 102
6.15 BACK UP AND DISASTER PLAN {8.15} (E) 103
6.16 SOLUTION ADMINISTRATION {8.16} (E) 107
6.17 HOSTING AND PROVISIONING {8.17} (E) 109
6.18 TRIAL AND TESTING PERIODS (PRE- AND POST- PURCHASE) {8.18} (E) 111
6.19 INTEGRATION AND CUSTOMIZATION {8.19} (E) 113
6.20 MARKETING PLAN {8.20} E) 116
6.21 RELATED VALUE-ADDED SERVICES TO CLOUD SOLUTIONS {8.21} (E) 117
6.22 SUPPORTING INFRASTRUCTURE {8.22} (E) 119
6.23 ALIGNMENT OF CLOUD COMPUTING REFERENCE ARCHITECTURE {8.23} (E) 120

Section 7 Confidential Protected, or Proprietary Information 121

Section 8 Exceptions and / or Additions to the Standard Terms and Conditions 123

Section 9 Cost Proposal {Separate Volume} 124

Attachment A: NASPO ValuePoint Master Agreement A-1

Attachment B: Explanation Cloud Security Alliance Questionnaires B-1

Attachment C: NIST Service Models C-1

Attachment D: Scope of Services D-1

Attachment E: Intent to Participate & State-Specific Terms and Conditions E-1

Attachment F: Intentionally Removed F-1

Attachment G: Cost Proposal Form (Separate Volume) G-1

Attachment H: Identification of Service Models H-1

Appendix A – Exception and/or Additions to the Standard Terms and Conditions..... A-A-1

Appendix B – CSA STAR Assessment A-B-1

Appendix C – VMware Terms and Conditions.....A-C-1

Appendix D – Resumes A-D-1

Appendix E – VMware Marketing Plan.....A-E-1

Appendix F – VMware Financial Solutions (VFS) A-F-1

Appendix G – Confidentiality Claim Form..... A-G-1

Compliance / Traceability Matrix

RFP Section Requirement	RFP Section Number	Response Section Number
Signature Page	5.1	Section 1
Cover Letter	5.2	Section 1
Acknowledgement of Amendments	5.3	Section 1
Executive Summary	5.4	Section 2
General Requirements for Service Offerings	5.5	Section 3
Recertification	5.8	Section 3.2
Business Profile	6.1	Section 4
Scope of Experience	6.2	Section 4.1
Financials	6.3	Section 4.2
Contract Manager	7.1	Section 4.3
Business Profile	6.1	Section 4
Scope of Experience	6.2	Section 4.1
General Information	6.4	Section 4.3
Billing and Pricing Practices	6.5	Section 4.4
Scope and Variety of Cloud Solutions	6.6	Section 4.5
Best Practices	6.7	Section 4.6
ORGANIZATION AND STAFFING	7	Section 5
Contract Manager	7.1	Section 5.1
TECHNICAL REQUIREMENTS	8	Section 6
Technical Requirements	8.1	Sections 6.1 - 6.19
Subcontractors	8.2	Section 6.2
Working with Purchasing Entities	8.3	Section 6.3
Customer Service	8.4	Section 6.4
Security of Information	8.5	Section 6.5
Privacy and Security	8.6	Section 6.6
Migration and Redeployment Plan	8.7	Section 6.7
Service of Data Recovery	8.8	Section 6.8
Data Protection	8.9	Section 6.9
Service Level Agreements	8.10.	Section 6.10
Data Disposal	8.11	Section 6.11
Performance Measures and Reporting	8.12	Section 6.12
Cloud Security Alliance Questionnaires	8.13	Section 6.13
Service Provisioning	8.14	Section 6.14

RFP Section Requirement	RFP Section Number	Response Section Number
Back up and Disaster Plan	8.15	Section 6.15
Solution Administration	8.16	Section 6.16
Hosting and Provisioning	8.17	Section 6.17
Trial and Testing Periods	8.18	Section 6.18
Integration and Customization	8.19	Section 6.19
Marketing Plan	8.20.	Section 6.20
Value-Added Services	8.21	Section 6.21
Supporting Infrastructure	8.22	Section 6.22
Alignment of Cloud Computing	8.23	Section 6.23
Confidential, Protected or Proprietary Information	3.12	Section 7
Exceptions and/or Additions to the standard Terms and Conditions	3.12	Section 8
Cost Proposal	3.12	Section 9

Section 1 Signature Page {5.1}

5.1 (M) SIGNATURE PAGE

Proposals must be submitted with a vendor information form, located on Bidsync as an attachment to the RFP, which must contain an ORIGINAL HANDWRITTEN signature executed in INK OR AN ELECTRONIC SIGNATURE, and be returned with the Offeror's proposal.

State of Utah Vendor Information Form

Legal Company Name (include d/b/a if applicable)	Federal Tax Identification Number	State of Utah Sales Tax ID Number	
VMware, Inc.	94-3292913	12510205-002-STC	
Ordering Address	**City**	**State**	**Zip Code**
3401 Hillview Ave	Palo Alto	CA	94304
Remittance Address (if different from ordering address)	**City**	**State**	**Zip Code**
27575 Network Place	Chicago	IL	60673-1275
Type ☐ Proprietorship ☐ Partnership ☐ Government ☒ For-Profit Corporation ☐ Non-Profit Corporation	Company Contact Person: Karin Whitwood		
Telephone Number (include area code): 571-375-3481	Fax Number (include area code): 650-475-5001		
Company's Internet Web Address: www.vmware.com	Email Address: kwhitwood@vmware.com		
Offeror's Authorized Representative's Signature: Luis A. Mata — Digitally signed by Luis A. Mata, DN: cn=Luis A. Mata, o=VMware, ou=Legal, email=lmata@vmware.com, c=US, Date: 2016.03.03 11:05:51 -08'00'			
Type or Print Name on behalf of: Michael Quinn			
Position or Title of Authorized Representative: Director, Americas Deals Desk			
Date: March 3, 2016			

RFP Administrative Information

RFP Title:	Cloud Solutions
RFP Project Description:	The State of Utah, in conjunction with NASPO ValuePoint, is seeking Contract Vendor(s) to provide cloud solutions as described in the RFP.
RFP Lead:	Christopher Hughes, Assistant Director State of Utah, Division of Purchasing christopherhughes@utah.gov (801) 538-3254
Submit sealed proposal (if submitting manually): MANUAL PROPOSALS MUST BE RECEIVED AT THE PHYSICAL ADDRESS DESIGNATED FOR COURIER SERVICE AND TIME/DATE STAMPED BY THE UTAH DIVISION OF PURCHASING PRIOR TO THE CLOSING DATE AND TIME. PROPOSALS RECEIVED AFTER THE DEADLINE, REGARDLESS OF REASON, WILL NOT BE REVIEWED. Submit electronically via Bidsync:	Address for Courier: State of Utah Division of Purchasing 3150 State Office Building, Capitol Hill Salt Lake City, Utah 84114-1061. Electronic Submission" www.bidsync.com
Question and Answer Period:	December 21, 2015 – January 29, 2016
RFP Closing Date:	March 10, at 1:00 pm MTN
Initial Term of Master Agreement and Renewals:	The term of the Master Agreement will be ten (10) years with no renewal periods. Upon mutual agreement, the Master Agreement may be extended or amended.
TAKE NOTE OF THE 0.25% NASPO VALUEPOINT ADMINISTRATIVE FEE WHICH MUST BE INCORPORATED INTO YOUR BASE PRICE. OTHER STATES, INCLUDING THE STATE OF UTAH, MAY NEGOTIATE ADDITIONAL ADMINISTRATIVE FEES IN THEIR PARTICIPATING ADDENDA FOLLOWING AWARD OF A MASTER AGREEMENT. The Request for Proposal contains the following Attachments and Exhibits: Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions Exhibit 1 to Attachment A: Software-as-a-Service Terms and Conditions Exhibit 2 to Attachment A: Platform-as-a-Service Terms and Conditions Exhibit 3 to Attachment A: Infrastructure-as-a-Service Terms and Conditions Attachment B: Explanation Cloud Security Alliance Questionnaires Exhibit 1 to Attachment B: Consensus Assessments Initiative Questionnaire Exhibit 2 to Attachment B: Cloud Controls Matrix Attachment C: NIST Service Models Attachment D: Scope of Services Attachment E: Intent to Participate & State-specific terms and conditions Attachment F: Intentionally Removed Attachment G: Cost Proposal Form Attachment H: Identification of Service Models	

This Request for Proposals ("RFP"), having been determined to be the appropriate procurement method to provide the best value to the State of Utah Division of Purchasing, is designed to provide interested Offerors with sufficient basic information to submit proposals. It is not intended to limit a proposal's content or exclude any relevant or essential data or information. Offerors are at liberty and are encouraged to expand upon the specifications to evidence capability to provide the cloud solutions requested in the RFP. The RFP is issued in accordance with State of Utah Procurement Code, Utah Code Annotated (UCA) Chapter 63G-6a, and applicable Rules found in the Utah Administrative Code (UAC). If any provision of this RFP conflicts with the UCA or UAC, the UCA or UAC will take precedence

VMware Response:

VMware has read and agrees.

2 General Information

This RFP is designed to provide interested Offerors with sufficient information to submit proposals meeting minimum requirements and technical qualifications.

2.1 Purpose

The State of Utah, Division of Purchasing (Lead State) is requesting proposals for cloud solutions in furtherance of the NASPO ValuePoint Cooperative Purchasing Program. The purpose of this Request for Proposals (RFP) is to establish Master Agreements with qualified Offerors to provide services related to cloud solutions for all Participating Entities. The objective of this RFP is to obtain best value, and achieve more favorable pricing, than is obtainable by an individual state or local government entity because of the collective volume of potential purchases by numerous state and local government entities. The Master Agreement(s) resulting from this procurement shall be extended to state governments (including departments, agencies, institutions), institutions of higher education, political subdivisions (i.e., colleges, school districts, counties, cities, etc.), the District of Columbia, territories of the United States, and other eligible entities subject to approval of the individual state procurement director and compliance with local statutory and regulatory provisions. The initial term of the Master Agreement shall be ten (10) years with no renewal provisions; however, Contract Vendors must submit an annual certification that they are still compliant with the mandatory minimum requirements and technical specification of the RFP.

Each state, territory, and participating entity is unique in how they currently employ cloud solutions; some are utilizing cloud solutions to augment services that their technology departments provide to end users and some have not entered the realm of outsourcing technical solutions to cloud solutions providers. This cooperative procurement effort's objective is to provide states, territories, and their authorized political subdivisions with high quality cloud based service providers that have the ability to provide a menu of cloud solutions offerings that will ultimately increase the technology department's overall efficiency, reduce costs, improve operational scalability, provide business continuity, increase collaboration efficiencies, and allow for expanded flexibility in work practices and system improvements.

The resulting Master Agreement contract(s) will provide Participating Entities with access to technical capabilities that run in cloud environments and meet the NIST Essential Characteristics. Sub-categories in scope are the three NIST Service Models, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

The awarded contracts will allow Participating Entities to choose cloud solutions that meet the following descriptions:

- Commercially available cloud computing services
- Meets the National Institute for Standards and Technology (NIST) definition of Cloud Computing

- Open to all deployment models (private, public, community or hybrid), vendors specify deployment models

VMware Response:

VMware has read and will comply with the requirements and specifications as mutually agreed upon under the resulting master agreement and its exhibits. As part of its offering, VMware will provide its portfolio of products and cloud services for customers that require private, public, hybrid, and community cloud options. This response proposes a best value solution which will provide Participating Entities with access to technical capabilities that run in cloud environments and meet the NIST Essential Characteristics as described herein. If awarded a contract, VMware will submit an annual certification that it is compliant with the mandatory minimum requirements and technical specifications of the RFP.

2.2 Lead State

The State of Utah Division of Purchasing is the Lead State and issuing office for this solicitation and all subsequent addenda relating to it. The reference number for the transaction is CH16012. This number must be referred to on all proposals, correspondence, and documentation relating to the RFP.

VMware Response:

VMware has read and agrees. VMware has and will continue to refer to transaction reference number CH16012 on all proposals, correspondence, and documentation relating to this RFP.

2.3 Definitions

The following definitions apply to the RFP. **Attachment A** contains the definitions of terms used in the NASPO ValuePoint Master Agreement Terms and Conditions. **Attachment D**, the Scope of Services, contains the definitions for the Service Models, Deployment Models and the NIST Essential Characteristics.

Contract Vendor means the Offeror awarded a Master Agreement by the Lead State. The Contract Vendor is the party responsible for delivering the Offerings under the terms and conditions set forth in the Master Agreement.

Eligible Users means every agency, political subdivision, or nonprofit that has the statutory authority to purchase from state cooperative contracts established by a Participating Entity to qualify for the cloud solutions described in the RFP. The Participating Entity will have sole discretion to determine who qualifies as an Eligible User.

Fulfillment Partner means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Solutions under this Master Agreement and billing Customers directly for such Solutions. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

Lead State means the State conducting this cooperative procurement, evaluation, and award.

Master Agreement means the underlying agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contract Vendor, as now or hereafter amended.

Offeror means the company or firm which submits a proposal in response to this Request for Proposal.

Participating Addendum means a written statement of agreement signed by the Contract Vendor and a Participating State or Participating Entity that clarifies the operation of the Master Agreement for the Participating Entity (e.g. ordering procedures specific to Participating State) and may add other state-specific language or other requirements. A Participating Addendum evidences the Participating Entity's willingness to purchase and the Contract Vendor's willingness to provide Offerings under the terms and conditions of the Master Agreement with any and all exceptions noted and agreed upon.

Participating State or Participating Entity means States that utilize the Master Agreement established by the RFP and enter into a Participating Addendum which further defines their participation.

Proposal means the official written response submitted by an Offeror in response to this Request for Proposal.

Purchasing Entity means any end-user in a Participating State (or other Participating Entity) that is eligible to use the Master Agreement(s) through the Participating Addendum.

Request for Proposals or RFP means the entire solicitation document, including all parts, sections, exhibits, attachments, and amendments.

Solutions or Offerings means deployment models (e.g. private, public, community, or hybrid) or the service model of cloud computing (e.g. IaaS, PaaS, SaaS, or a combination thereof), that most closely describes the Offeror's offering for the RFP.

Subcontractor means any organization, whether designated as a subcontractor, fulfillment partner, reseller, etc., that will assist an Offeror to provide an Offering if awarded a Master Agreement.

VMware Response:

VMware has read and will comply with the requirements and specifications as mutually agreed upon under the resulting master agreement and its exhibits.

2.4 NASPO ValuePoint Background Information

NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

VMware Response:

VMware has read and agrees.

2.5 Participating States

In addition to the Lead State conducting this solicitation, the following Participating States have requested to be named in the RFP as potential participating entities on the resulting Master Agreement: See **Attachment E**. Other entities may become Participating Entities after award of the Master Agreement.

State-specific terms and conditions that will govern each state's Participating Addendum are included in **Attachment E,** and/or may be incorporated into the Participating Addendum after award.

Additional States may be added with the consent of the awarded Contract Vendor and the Lead State (on behalf of NASPO ValuePoint) through execution of a Participating Addendum.

VMware Response:

VMware has read and agrees.

2.6 Anticipated Usage

This is a new service for the Lead State and NASPO ValuePoint. Therefore, annual usage data is not available. Usage will be dependent on the needs of each Participating Entity. No minimum or maximum level of sales volume is guaranteed or implied in awarded Master Agreements awarded under the RFP.

VMware Response:

VMware has read and agrees.

2.7 Terms and Conditions Governing Solicitation and Resulting Agreements

2.7.1 **Solicitation**

The solicitation consists of the RFP document, including all Exhibits and Attachments listed on Bidsync.

2.7.2 **Master Agreement**

The Master Agreement(s) awarded from this RFP will consist of the negotiated Master Agreement Terms and Conditions, the relevant Scope of Services, the Offeror's Cost Proposal form, and the winning Offeror's Proposal as revised (if permitted) and accepted by the Lead State.

2.7.3 **Participating Addenda**

Participating Entities, including the State of Utah, may negotiate additional and/or different terms and conditions in a Participating Addendum, which will take precedence over the terms of the Master Agreement in the event of conflict. Participating Entities may not negotiate the addition of services not contemplated by this RFP.

VMware Response:

VMware has read and agrees.

2.8 Contract Award

It is anticipated that the RFP will result in multiple contract awards established by the multiple award methodology.

The multiple award methodology: All offerors that meet/exceed the technical minimum scoring thresholds and all solicitation minimum requirements will be eligible for award - subject to successful terms and conditions negotiations. Participating Entities and Eligible Users may base their "best value" selection of the offeror whose qualifications best meet their needs after reviewing qualifications outlined in the offeror's proposal and considering other information in the solicitation process relevant to their determination of best value (such as the proposals and evaluations).

The awarded Master Agreement(s) may be modified as a result of technological upgrades for the procurement item(s). Any modification for upgraded technology must be substantially within the scope of the original procurement or contract, and if both parties agree to the modification, then the contract may be modified, but it may not extended beyond the term of the original awarded contract unless otherwise permitted by law. The awarded contract(s) may be modified for new technology related to the procurement item(s).

Open-Ended Procurement: Pursuant to Part 4 and 7 of the Utah Procurement Code, it is the intent of the RFP to be for ten years with recertification of the Contract Vendors on an annual basis, as required by Section 5.8. A Contract Vendor's failure to recertify will result in the termination of its Master Agreement.

In addition, on a biennial basis the Lead State may re-issue a solicitation, using this RFP document, to solicit new vendors that can provide additional Cloud Solutions to Participating Entities and Purchasing Entities.

VMware Response:

VMware has read and agrees.

2.9 Scope of Services

The Scope of Services is provided in **Attachment D.** To meet the requirements of many of the Participating Entities the Scope of Services was modeled after NIST, including any definitions, security controls, and mechanisms for implementation. Participating Entities may have to modify definitions and terms in order to comply with federal, state, and local laws, regulations, and guidelines. Proposals should demonstrate their compliance with the standards set forth in **Attachment D**.

VMware Response:

VMware has read and will comply with the requirements and specifications as mutually agreed upon under the resulting master agreement and its exhibits.

2.10 Choice of Law, Solicitation Jurisdiction, and Venue

The provisions of the RFP and all matters, including any dispute or protest, in regard to the RFP that occur prior to the full execution of any contract resulting from the RFP, shall be governed by the laws of the State of Utah. The parties will submit to the jurisdiction of the courts of the State of Utah for any dispute arising out of the RFP or any matter related thereto prior to the full execution of the awarded contract(s). Venue for said dispute or protest shall be in Salt Lake City, in the Third Judicial District Court for Salt Lake County. The provisions of the Utah Procurement Code, Title 63G, Chapter 6a, and Utah Administrative Code Rules R33 must be met in regard to any protest. The substantially successful party, including any intervening parties, shall be entitled to their reasonable attorney fees and costs being paid by the substantially unsuccessful party(ies). This paragraph shall not supersede any provision related to a purchasing entity outside the State of Utah.

VMware Response:

VMware has read agrees.

2.11 Other Value-Added Services

Offerors may propose other Value-Added Services in their response. Such services from an awarded Offeror, if consistent with this Scope of Services, recommended by the Evaluation Team, and accepted by the Lead State, would be added to the final awarded contract.

VMware Response:

As part of our response, VMware is proposing value added services available to the State of Utah and participating states under the contract.

Please refer to section 6.21 of our proposal for VMware's proposed value added services.

2.12 Service Line Additions and Updates

During the term of the Master Agreement(s), Offerors may submit a request to update the awarded Solutions as services are introduced or removed from the Offeror's offerings. The Master Agreement Administrator will evaluate requests and update the contract offering via written amendment as appropriate. The Offerors shall update the dedicated website, price lists, and catalogs to reflect approved changes. Pricing must utilize the same pricing structure as was used for services falling into the same service category.

VMware Response:

VMware has read and agrees.

2.13 Additional Sources

In the best interest of the states involved, NASPO ValuePoint, Participating States, and Purchasing Entities reserve the right to competitively solicit additional sources for these commodities during the contract term. Further, Participating States may have existing awards for commodities with the scope of the RFP.

VMware Response:

VMware has read and agrees.

2.14 NASPO ValuePoint eMarket Center

The awarded cloud service contractors will not have any type of catalog within the eMarket Center, they will have Ordering Instructions. These instructions provide visibility to the contractor within the eMarket Center as well as provide information about the contractor and how to order directly from the contractor, outside of the eMarket Center.

In July 2011, NASPO ValuePoint entered into a multi-year agreement with SciQuest, Inc. whereby SciQuest will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provided customers information regarding the Contractors website and ordering information.

At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the customer to have.

VMware Response:

VMware has read and agrees.

3 Solicitation Requirements, Information and Instructions

3.1 Question and Answer PERIOD

The RFP is issued by the State of Utah Division of Purchasing via Bidsync. The Division of Purchasing is the only contact for this solicitation. Do not contact any other Participating Entity about the RFP.

All questions MUST be submitted through BIDSYNC (www.bidsync.com) during the designated time for questions ("Q&A period") listed on Bidsync. Questions submitted through any other channel will not be answered. Questions may be answered in the order that they are submitted or may be compiled into one document and answered via an addendum. Answers disseminated by the State through the BidSync system shall serve as the official and binding position of the State and will constitute an addendum to this RFP.

Questions, exceptions, or notification to the State of any ambiguity, inconsistency, excessively restrictive requirement, or error in this RFP, MUST be submitted as a question through BidSync during the Q&A period.

Questions may be answered individually or may be compiled into one document. Questions may also be answered via addenda. An answered question or addenda may modify the specification or requirements of this RFP. Answered questions and addendums will be posted on BidSync. Offerors should periodically check BidSync for answered questions and addendums before the closing date. It is the responsibility of the Offerors to submit their proposal as required by this RFP, including any requirements contained in an answered question and/or addendums.

Exceptions to scope/content of the RFP within an Offeror's proposal that have not been previously addressed within the Q&A period of the procurement are not allowed and may result in the Offeror's proposal being considered non-responsive.

VMware Response:

VMware has read and agrees.

3.2 ADDENDUMS

Offerors are encouraged to periodically check BidSync for posted questions, answers and addendums. Offerors will not be notified by the Lead State or Bidsync for each addendum issued under the RFP.

Any modification to this procurement will be made by addendum issued by the Lead State. Addendums to the RFP may be made for the purpose of making changes to: the scope of work, the schedule, the qualification requirements, the criteria, the weighting, or other requirements of the RFP.

After the due date and time for submitting a proposal to the RFP, at the discretion of the Lead State, addenda to the RFP may be limited to the Offerors that have submitted proposals, provided the addenda

does not make a substantial change to the RFP that likely would have impacted the number of Offerors responding to the original publication of the RFP, in the opinion of the Lead State.

Authorized and properly issued addenda shall constitute the official and binding position of the State.

Any response to the RFP which has as its basis any communications or information received from sources other than the RFP or related addenda may be considered non-responsive and be rejected at the sole discretion of the State.

VMware Response:

VMware has read and agrees.

3.3 RESTRICTIONS ON COMMUNICATIONS

From the issue date of the RFP until the contract award(s), Offerors are prohibited from communications regarding the RFP with other Participating Entities EXCEPT the Lead State. Failure to comply with this requirement may result in disqualification.

VMware Response:

VMware has read and agrees.

3.4 Exceptions to RFP and NASPO ValuePoint Master Agreement Terms and Conditions

Any contract resulting from this RFP will include the NASPO ValuePoint Master Agreement Terms and Conditions (Master Agreement Terms and Conditions), Attachment A, including Exhibits to Attachment A.

Exceptions and/or additions to the Master Agreement Terms and Conditions and other requirements of this RFP are strongly discouraged. Any exception and/or addition regarding the **Master Agreement Terms and Conditions** must be made in the Offeror's proposal. The Lead State will not consider proposed modifications and/or additions to the Master Agreement Terms and Conditions after the deadline for proposals. Exceptions and/or additions regarding the Master Agreement Terms and Conditions or other RFP provisions must contain the following:

1. The rationale for the specific requirement being unacceptable to the Offeror submitting the exception and/or addition;
2. Recommended verbiage for the Lead State's consideration that is consistent in content, context, and form with the Master Agreement Terms and Conditions;
3. Explanation of how the Lead State's acceptance of the recommended verbiage is fair and equitable to both the Lead State, the Participating Entities, and to the Offeror submitting the modification and/or exception.

Offerors may not submit requests for exceptions and/or additions by reference to an Offeror's website or URL. URLs provided with a proposal may result in that proposal being rejected as non-responsive. Offerors may submit questions during the Q&A period regarding the Master Agreement Terms and Conditions.

The Lead State may refuse to negotiate exceptions and/or additions that are determined to be excessive; that are inconsistent with similar contracts; and to warranties, insurance, or indemnification provisions that are necessary to protect the procurement unit after consultation with the Attorney General's Office or other applicable legal counsel, including a Participating Entity.

For the RFP, the Lead State reserves the right to negotiate exceptions and/or additions to terms and conditions in a manner resulting in expeditious resolutions. This process may include beginning negotiations with the qualified Offeror having the least amount of exceptions and/or additions and concluding with the Offeror submitting the greatest number of exceptions and/or additions. Contracts may be executed and become effective as negotiations are completed; however, all of the resulting Master Agreement(s) will terminate on the same date.

If negotiations are required, Offeror must provide all documents in Microsoft Word format for redline editing. Offeror must also provide the name, contact information, and access to the person(s) that will be directly involved in legal negotiations.

An award resulting from the RFP is subject to successful contract terms and conditions negotiation (if required). The Lead State, at its sole discretion, will determine when contract terms and conditions negotiations become unproductive and will result in termination of award to that Offeror.

VMware Response:

VMware has read and provides a response to exceptions in Section 8 to explain our understanding and approach. Additionally, we have prepared an exceptions/clarification chart which may be found in **Appendix A** and provides the additional detail requested for exceptions in accordance with the specifications provided in this RFP section 3.4. VMware respectfully reserves the right to negotiate the terms and conditions of the Master Agreement as provided in the solicitation to appropriately reflect applicable commercial industry standards and government requirements for the circumstances of the solutions included. We are confident that we can reach a mutually agreeable agreement as we have in previous situations with public sector entities.

3.5 Proposal Due Date

Proposals must be received by the closing date and time as described on Bidsync. Proposals received after the deadline will not be accepted.

VMware Response:

VMware has read and agrees.

3.6 Cancellation of Procurement

The RFP may be canceled at any time prior to award of the Master Agreement(s), if the Lead State determines such action to be in the collective best interests of potential Participating States.

VMware Response:

VMware has read and agrees.

3.7 Governing Laws and Regulations

The RFP is conducted by the Lead State, in accordance with its procurement code and applicable administrative rules, which can be found in Utah Code, Utah Administrative Code, and other policies, available at: http://purchasing.utah.gov/.

This procurement shall be governed by the laws and regulations of the Lead State. Venue for any administrative or judicial action relating to the RFP, evaluation, and award shall be in Salt Lake County,

Utah. The provisions governing choice of law and venue for issues arising after award and during contract performance are specified in **Attachment A**.

VMware Response:

VMware has read and agrees.

3.8 Intentionally Deleted.

VMware Response:

VMware acknowledges.

3.9 Right to Accept All or Portion of Proposal

Unless otherwise specified in the solicitation, the Lead State may accept any Offering or combination of Offerings as specified in the solicitation or of any proposal.

VMware Response:

VMware has read and agrees.

3.10 Proposal Content and Format Requirements

Include a Table of Contents in the Proposal identifying the contents of each section, including page numbers of major sections. Proposals should follow the numerical order of the RFP starting at the beginning and continuing through the end of the RFP. Proposal sections and subsections shall be identified with the corresponding numbers and headings used in the RFP. In your response, restate the RFP section and/or subsection, followed with your response. Offerors are encouraged to use a different color font, bold text, italics, or other indicator to clearly distinguish the RFP section or subsection from the Offeror's response.

Proposals must be detailed and concise. The format is designed to ensure a complete submission of information necessary for an equitable analysis and evaluation of submitted proposals. There is no intent to limit the content of proposals; however, technical responses must focus on responding to the RFP and should not include preprinted advertising materials.

VMware Response:

VMware has read and agrees.

3.11 Proposal Submission Instructions

Proposals may be submitted manually or electronically. **Proposals must be submitted as described in Section 3.10.**

3.11.1 Electronically Submitted Proposals

Electronically submitted proposals must be submitted through Bidsync, the Lead State's eProcurement provider, at www.bidsync.com. When submitting through Bidsync, enter your "Total Cost" in Bidsync as "$0," and **UPLOAD YOUR** SEPARATE **TECHNICAL PROPOSAL, COST PROPOSAL AND ALL OTHER REQUIRED DOCUMENTS**, including your signed State of Utah Signature Page.

Electronic proposals may require uploading of electronic attachments. BidSync will accept a wide variety of document types as attachments. However, the State is unable to view certain attachments. Therefore, DO NOT submit attachments that are embedded (zip files), movies, wmp, encrypted, or mp3 files. All attachments must be uploaded in BidSync as separate files. All attachments shall be submitted in a format acceptable to the Lead State. Acceptable formats include .doc (Microsoft Word document), .xls (Microsoft Excel spreadsheet), and .pdf (Adobe Acrobat portable document format).

Be advised that the "Offeror" for bid evaluation and award purposes is the entity profile you submit under in Bidsync, which must be the same legal entity presented in your attached response materials. Your submission via Bidsync is your electronic signature, acknowledging the statements contained in the State of Utah Signature Page.

Offerors are further advised to upload response materials with descriptive file names, organized and consolidated in a manner which allows evaluators to efficiently navigate their response; as the Lead State will print uploaded documents for evaluation in the manner received via Bidsync.

3.11.2 Manually Submitted Proposals

Manually submitted proposals must be addressed to the RFP Lead and must be sealed and identified as "**CH16012 – Cloud Solutions**." The Technical Proposal and separately sealed Cost Proposal must be submitted at the same time (place all proposal response materials within a larger package).

The Technical portion of the Proposal must be clearly marked "TECHNICAL PROPOSAL – CH16012 - Cloud solutions."

Each proposal must be submitted in one (1) original with eight (8) copies of the Technical Proposal and one (1) original and one (1) copy of the Cost Proposal.

Offerors submitting manually must also submit one (1) electronic copy of the proposal on CD or USB device. Word or Excel format is required (the only exception is for financials, brochures or other information only available in an alternate format). The format and content must be the same as the manually submitted proposal. The electronic version must NOT be password protected or locked in any way.

Offeror should allow sufficient time for delivery of hardcopy proposals. Proposals sent overnight, but not received by the deadline time will not be accepted. When submitting a proposal by physical delivery (U.S. Mail, courier service, hand-delivery, or other physical means), Offerors are solely responsible for meeting the deadline. Delays caused by a delivery service or other physical means will not be considered as an acceptable reason for a proposal being late. All proposals received by physical delivery will be date and time stamped by the Lead State.

If your proposal, whether electronically or manually submitted, contains proprietary or confidential information which you have identified, you must also submit a redacted copy of the Technical Proposal (in electronic format, with the word "redacted" in the file name) with all proprietary or confidential information removed or blacked out; as well as a separate document containing a complete list (per the instructions in Subsection 3.11, below) of all trade secret information which was removed or blacked out in the redacted copy.

3.11.3 Cost proposal will be evaluated independently from the technical proposal, pursuant to Utah Code Annotated (UCA) § 63G-6-707(5), and as such, must be submitted separate from the technical proposal. Failure to submit cost or pricing data separately may result in your proposal being judged as non-responsive and ineligible for contract award. The Cost Proposal must be separately sealed and identified as "**Cost Proposal –CH16012 Cloud solutions**."

VMware Response:

VMware has read and agrees.

3.12 SUBMISSION OF PROPOSAL

By submitting a proposal to the RFP, the Offeror acknowledges and agrees that the requirements, scope of work, and the evaluation process outlined in the RFP are understood, fair, equitable, and are not unduly restrictive. Any exceptions to the content of the RFP, excluding the Master Agreement Terms and Conditions contained in Attachment A, including the Exhibits to Attachment A, must be addressed within the Q&A period. The Offeror further acknowledges that it has read the RFP, along with the Exhibits, Attachments, and any attached or referenced documents, including the General Provisions.

All Proposals must be submitted in the following format. Offerors should title each document with the names listed below. Proposals may be submitted as one document with a separately attached Cost Proposal form or as individual documents. If an Offeror submits a redacted version of a document it should clearly label the document as redacted. Detailed information on submitting each of these sections is contained later sections of this RFP.

1. **Section Title: RFP Signature Page.** The Lead State's Request for Proposal Signature Page completed and signed. See Section 5.1 of the RFP.
2. **Section Title: Executive Summary.** The one or two page executive summary is to briefly describe the Offeror's Proposal. This summary should highlight the major features of the Proposal. It must indicate any requirements that cannot be met by the Offeror. The Lead State should be able to determine the essence of the Proposal by reading the executive summary. See Section 5.4 of the RFP.
3. **Section Title: Mandatory Minimums:** This section should constitute the Offeror's point-by-point response to each item described in Section 5 of the RFP, except 5.1 (Signature Page) and 5.4 (Executive Summary). An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 5 of the RFP.
4. **Section Title: Business Profile:** This section should constitute the Offeror's response to the items described in Section 6 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 6 of the RFP.
5. **Section Title: Organization Profile:** This section should constitute the Offeror's response to the items described in Section 7 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 7 of the RFP.
6. **Section Title: Technical Response.** This section should constitute the Technical response of the proposal and must contain at least the following information:

A. A complete narrative of the Offeror's assessment of the Cloud Solutions to be provided, the Offerors ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the Offeror's understanding of the desired overall performance expectations and clearly indicate any options or alternatives proposed.

B. A specific point-by-point response, in the order listed, to each requirement in the Section 8 of the RFP. Offerors should not provide links to a website as part of its response.

Offeror's should focus their proposals on the technical qualifications and capabilities described in the RFP. Offerors should not include sales brochures as part of their response.

7. **Section Title: Confidential, Protected or Proprietary Information.** All confidential, protected or proprietary Information must be included in this section of proposal response. Do not incorporate

protected information throughout the Proposal. Rather, provide a reference in the proposal response directing Lead State to the specific area of this protected Information section.

If there is no protected information, write "None" in this section.

Failure to comply with this Section and Section 3.13 of the RFP releases the Lead State, NASPO ValuePoint, and Participating Entities from any obligation or liability arising from the inadvertent release of Offeror information.

8. **Section Title: Exceptions and/or Additions to the Standard Terms and Conditions.** Proposed exceptions and/or additions to the Master Agreement Terms and Conditions, including the exhibits, must be submitted in this section. Offeror must provide all proposed exceptions and/or additions, including an Offeror's terms and conditions, license agreements, or service level agreements in Microsoft Word format for redline editing. Offeror must also provide the name, contact information, and access to the person(s) that will be directly involved in terms and conditions negotiations.

If there are no exceptions or additions to the Master Agreement Terms and Conditions, write "None" in this section.

9. **Section Title: Cost Proposal.** Cost Proposals will be evaluated independently from the technical proposal. Offeror's cost proposal must include the items discussed in Section 9 of the RFP.

Cost will be evaluated independently from the Mandatory Minimum Requirements, and the Technical responses. Inclusion of any cost or pricing data within the Detailed Technical Proposal will result in the proposal being judged as non-responsive for violation of UCA § 63G-6a-707(5).

All costs incurred by an Offeror in the preparation and submission of a proposal, including any costs incurred during interviews, oral presentations, and/or product demonstrations are the responsibility of the Offeror and will not be reimbursed by the Lead State or NASPO ValuePoint.

VMware Response:

VMware has read and agrees to the proposal submission format as detailed in this RFP section 3.12. VMware has provided a response to exceptions in Section 8 of this proposal and additionally identified specific terms and conditions within Attachment A – Master Agreement and its Exhibits to which VMware has provided suggested revisions as detailed in the chart found in **Appendix A** of this proposal response. VMware will comply with the requirements and specifications as mutually agreed upon under the resulting master agreement and its exhibits.

3.13 CONFIDENTIAL OR PROPRIETARY INFORMATION

The Government Records Access and Management Act (GRAMA), UCA § 63G-2-305, provides in part that:

the following records are protected if properly classified by a government entity:

(1) trade secrets as defined in Section 13-24-2, the Utah Uniform Trade Secrets Act, if the person submitting the trade secret has provided the governmental entity with the information specified in UCA § 63G-2-309 (Business Confidentiality Claims);

(2) commercial information or non-individual financial information obtained from a person if:

(a) disclosure of the information could reasonably be expected to result in unfair competitive injury to the person submitting the information or would impair the ability of the governmental entity to obtain necessary information in the future;

(b) the person submitting the information has a greater interest in prohibiting access than the public in obtaining access; and

(c) the person submitting the information has provided the governmental entity with the information specified in UCA § 63G-2-309;

* * * * *

(6) records, the disclosure of which would impair governmental procurement proceedings or give an unfair advantage to any person proposing to enter into a contract or agreement with a governmental entity, except, subject to Subsections (1) and (2), that this Subsection (6) does not restrict the right of a person to have access to, after the contract or grant has been awarded and signed by all parties, ...

Pricing may not be classified as confidential or protected and will be considered public information after award of the contract.

Process for Requesting Non-Disclosure: Any Offeror requesting that a record be protected shall include with the proposal a Claim of Business Confidentiality. To protect information under a Claim of Business Confidentiality, the Offeror must complete the Claim of Business Confidentiality form with the following information:

1. Provide a written Claim of Business Confidentiality at the time the information (proposal) is provided to the state, and

2. Include a concise statement of reasons supporting the claim of business confidentiality (UCA § 63G-2-309(1)).

3. Submit an electronic "redacted" (excluding protected information) copy of the record. The redacted copy must clearly be marked "Redacted Version."

The Claim of Business Confidentiality Form may be accessed at:

http://www.purchasing.utah.gov/contract/documents/confidentialityclaimform.doc

An entire proposal cannot be identified as "PROTECTED", "CONFIDENTIAL" or "PROPRIETARY", and if so identified, shall be considered non-responsive unless the Offeror removes the designation.

Redacted Copy: If an Offeror submits a proposal that contains information claimed to be business confidential or protected information, the Offeror must submit two separate proposals: one redacted version for public release, with all protected business confidential information either blacked-out or removed, clearly marked as "Redacted Version"; and one non-redacted version for evaluation purposes, clearly marked as "Protected Business Confidential."

The Lead State and NASPO ValuePoint are not liable or responsible for the disclosure of any confidential or proprietary information if the Offeror fails to follow the instructions of this section.

VMware Response:

VMware has read and agrees.

3.14 ERRORS IN PROPOSALS

Pursuant to UAC R33-7-403, the following shall apply to the correction or withdrawal of an unintentionally erroneous proposal, or the cancellation of an award or contract that is based on an unintentionally erroneous proposal. A decision to permit the correction or withdrawal of a proposal or the cancellation of an award or a contract shall be supported in a written document, signed by the chief procurement officer or head of a procurement unit with independent procurement authority.

(1) Mistakes attributed to an offeror's error in judgment may not be corrected.

(2) Unintentional errors not attributed to an offeror's error in judgment may be corrected if it is in the best interest of the procurement unit and correcting the error maintains the fair treatment of other offerors.

(a) Examples include:

(i) missing signatures;

(ii) missing acknowledgement of an addendum;

(iii) missing copies of professional licenses, bonds, or insurance certificates, provided that copies are submitted by the deadline established by the chief procurement officer or head of a procurement unit with independent procurement authority to correct this mistake;

(iv) typographical errors;

(v) mathematical errors not affecting the total proposed price; or

(vi) other errors deemed by the chief procurement officer or head of a procurement unit with independent procurement authority to be immaterial or inconsequential in nature.

(3) Unintentional errors discovered after the award of a contract may only be corrected if, after consultation with the chief procurement officer or head of a procurement unit with independent procurement authority and the attorney general's office or other applicable legal counsel, it is determined that the correction of the error does not violate the requirements of the Utah Procurement Code or applicable administrative rules.

VMware Response:

VMware has read and agrees.

3.15 E-RATE

To the extent the services offered are subject to the E-rate discount program, all award Contract Vendors must commit to participation in the Federal Communication Commission's E-rate discount program established under authority of the Federal Telecommunications Commission Act of 1996. Participation in, and implementation of, this program must be provided without the addition of any service or administration fee by the Contract Vendor.

In order to participate in E-Rate Offerors must appear on the USAC website as those who have a Service Provider Identification Number or "SPIN."

VMware Response:

VMware commits to participation in the Federal Communication Commission's E-rate program. Our participation in the program is provided without the addition of any service or administrative fee for offering E-rate products.

VMware offers E-rate complaint products. It's our intent to use our authorized resellers for fulfilment of VMware products under this contract. When adding authorized resellers under our contract, we will identify them for their USAC SPIN, as applicable. Only authorized resellers with a USAC provided SPIN will be eligible to fulfil eRate funded opportunities.

Provided in **Table 1** below is the USAC SPIN for the resellers that we are in consideration to use under the contract, as finally awarded. Please see section 6.2 of this proposal response for a more detailed description regarding subcontractors.

VMware Reseller Name	USAC SPIN
Advanced Network Management	143028101
Advanced Systems Group	143026742
Advizex	143034901
Alexander Open Systems	143004953
Atrion	143004541
CDI	143037195
Dimension Data	143027251
Dyntek	143004427
En Pointe/PCMG	143006068
ePlus	143006553
GKR Systems, Inc. dba Venture Technologies	143008980
GovC	143026005
Insight Public Sector, Inc.	143030052
ISC, Inc. dba Venture Technologies	143012405
NWN	143024187
Presidio	143024659
Promedia	143004851
Zones	143030023

Table 1. E-rate SPIN for VMware Authorized Resellers

4 Evaluation and Award

4.1 Initial Review of Proposals

4.1.1 All proposals will be reviewed first to ensure that they meet the Mandatory Submission Requirements of the RFP as addressed in Sections noted with an (M). Any proposal(s) not meeting the Mandatory Submission Requirements may be found non-responsive.

VMware Response:

VMware has read and agrees.

4.1.2 The Technical Proposal will be evaluated first as either "pass" or "fail," based on compliance with those requirements listed in the RFP with an (M), (ME), or (E). All proposals which are determined to be responsive will continue in the evaluation process outlined in this section.

(M) means that the requirement is mandatory and a proposal must contain a response to that requirement; however, the proposal response is not evaluated. This is a pass/fail requirement as described in 4.3.1. The majority of these responses will require that the Offeror warrant or represent that it meets a certain

requirement[1]. Offerors are encouraged to demonstrate compliance with a mandatory minimum and to demonstrate that they meet or exceed to the requirement.

(ME) means that the requirement is both mandatory, as mentioned above will be reviewed in 4.3.1, and the proposal response will be evaluated and given a score under 4.3.2. If an Offeror's proposal does not address the requirement then it will fail and therefore be disqualified.

(E) means that the proposal response will be evaluated as described in 4.3.2.

VMware Response:

VMware has read and agrees.

4.2 Right to Waive Minor Irregularities

The State of Utah Chief Procurement Officer reserves the right to waive minor informalities as well as minor deviations. The Lead State also reserves the right to seek clarification on any proposal response.

VMware Response:

VMware has read and agrees.

4.3 Evaluation Process

In responding to this RFP, Offerors must identify and describe all of the Solutions that are contained in their proposals.

4.3.1 In the initial phase of the evaluation process, the Lead State will review all proposals timely received. Mandatory and scored on a pass/fail basis. A "Fail" will result in a proposal being deemed non-responsive and, therefore, will be disqualified. Failure to provide a response to each Mandatory requirement where indicated will result in disqualification.

Non-responsive proposals not conforming to the RFP requirements or unable to meet the mandatory minimum requirements will be eliminated from further consideration. The Offerors that meet the requirements and meet the mandatory minimum requirements will move on to the technical evaluation of their proposals.

Mandatory Minimum Requirements	RFP Section	Pass/Fail
Signature Page	5.1	Pass/Fail
Cover Letter	5.2	Pass/Fail
Acknowledgement of Amendments	5.3	Pass/Fail
Executive Summary	5.4	Pass/Fail
General Requirements	5.5	Pass/Fail
Re-Certification	5.7	Pass/Fail
Business Profile	6.1	Pass/Fail
Scope of Experience	6.2	Pass/Fail

[1] The Lead State reserves the right to verify that an Offeror's proposal meets the mandatory requirement.

Financials	6.3	Pass/Fail
Contract Manager	7.1	Pass/Fail
Cost Proposal Submitted	9.1	Pass/Fail

4.3.2 Evaluation of the Proposals will be evaluated and scored by an Evaluation Committee. It is anticipated that several Evaluation Committees will be established in order to evaluate all of the proposals in a reasonable amount of time. Proposals will be scored on the following evaluation criteria:

Evaluation Criteria	RFP Section	Points Possible
BUSINESS INFORMATION	6	
Business Profile	6.1	25.0
Scope of Experience	6.2	25.0
General Information	6.4	25.0
Billing and Pricing Practices	6.5	25.0
Scope and Variety of Cloud Solutions	6.6	25.0
Best Practices	6.7	25.0
ORGANIZATION AND STAFFING	7	
Contract Manager	7.1	25.0
TECHNICAL REQUIREMENTS	8	
Technical Requirements	8.1	50.0
Subcontractors	8.2	50.0
Working with Purchasing Entities	8.3	50.0
Customer Service	8.4	50.0
Security of Information	8.5	50.0
Privacy and Security	8.6	50.0
Migration and Redeployment Plan	8.7	50.0
Service or Data Recovery	8.8	50.0
Data Protection	8.9	50.0
Service Level Agreements	8.10	50.0
Data Disposal	8.11	50.0
Performance Measures and Reporting	8.12	50.0
Cloud Security Alliance	8.13	50.0
Service Provisioning	8.14	50.0
Back up and Disaster Plan	8.15	50.0
Solution Administration	8.16	50.0
Hosting and Provisioning	8.17	50.0
Trial and Testing Periods	8.18	50.0

Integration and Customization	8.19	50.0
Marketing Plan	8.20.	50.0
Value-Added Services	8.21	50.0
Supporting Infrastructure	8.22	50.0
Alignment of Cloud Computing	8.23	50.0

Offerors must receive a minimum score of seventy percent (70%) of the total possible points in order to continue to the scoring the cost proposals. Offerors with a score of less than seventy percent (70%) of the total possible points will be deemed non-responsive and ineligible for further consideration. If an Offeror demonstrates that an evaluation criteria is not applicable to its Offering then those points will be deducted from that Offerors total possible points. For example if an Offeror demonstrates that the evaluation criteria for Privacy and Security in Section 8.6 of this RFP is not applicable to its proposal then 50 points will be removed from that Offeror's total possible points (from 1325 to 1275). The Lead State reserves the right to determine whether an evaluation criteria applies to a proposal.

Offerors that achieve minimum score threshold of seventy percent (70%) of the total possible points, will proceed to the Cost Proposal Evaluation. The evaluation score sheet has been attached to this RFP. The attached evaluation score sheet states the relative weight that will be given to each evaluation criteria.

Each committee member shall independently read and score each proposal based on the technical non-price criteria set forth in the RFP to assess the completeness, quality, and desirability of each proposal. The Evaluation Committee will tally the final scores for criteria other than cost to arrive at a consensus score by the following method: an average of the individual scores. Each proposal will be evaluated and scored by at least three evaluation committee members.

To clarify, an Offeror's Cloud Solutions (SaaS, IaaS, or PaaS) are not being tested or demonstrated during the technical response; proposals are only being evaluated by the criteria described in the RFP. However, Purchasing Entities in making a "best value" determination may request a test or demonstration of an Offeror's Solution. To help in the evaluation process Offerors should not include sales brochures as part of their proposals.

4.3.3 Cost Proposals will be opened only after Evaluation of Proposals has been completed. Offerors that provide a price schedule with a minimum discount from its Cloud Solutions will receive 152.8 points. If an Offeror fails to provide a discount or a price schedule as required by Section 9.1 its proposal will be disqualified.

VMware Response:

VMware has read and agrees.

4.4 Award of Master Agreement(s)

Award shall be made to the responsive responsible Offeror(s) whose proposal(s) receive the minimum point thresholds and provides a Cost Proposal form as described in Section 4.3.3. The Lead State anticipates awarding multiple Master Agreements. The award of Master Agreement(s) will be made without regard to any preference for Utah suppliers. Participating Entities, including the State of Utah, may take local preferences into consideration when determining if they will enter into a Participating Addendum with a Contract Vendor to which a Master Agreement has been awarded.

VMware Response:

VMware has read and agrees.

4.5 Notice of Intent to Award

After final selections are made, the Lead State will issue an intent-to-award announcement by letter to all responsive Offerors.

VMware Response:

VMware has read and agrees.

4.6 PROTEST Processes

Offerors are directed to Utah Code Part 16 and Utah Administrative Code Rule R16 available at http://le.utah.gov/xcode/Title63G/Chapter6a/63G-6a-S1601.html and http://www.rules.utah.gov/publicat/code/r033/r033-016.htm for available protest processes.

VMware Response:

VMware has read and agrees.

4.7 PUBLICIZING AWARD(S)

The Lead State shall, on the next business day after the award of a contract(s) is announced, make available to each Offeror and to the public a written statement that includes:

(a) the name of the offeror to which the contract is awarded and the total score awarded by the evaluation committee to that offeror;

(b) the justification statement under UCA § 63G-6a-708, including any required cost-benefit analysis; and

(c) the total score awarded by the evaluation committee to each offeror to which the contract is not awarded, without identifying which offeror received which score.

VMware Response:

VMware has read and agrees.

Cover Letter {5.2}

VMware, Inc.

Public Sector:
12100 Sunset Hills Dr.
Reston, VA 20190
www.vmware.com

Company Headquarters:
3401 Hillview Avenue
Palo Alto, CA 94304

Christopher Hughes, Assistant Director
State of Utah, Division of Purchasing
3150 State Office Building, Capitol Hill
Salt Lake City, Utah 84114-1061
Submitted electronically via www.bidsync.com

RE: NASPO ValuePoint in conjunction with the State of Utah, Request for Proposals (RFP), UT solicitation No. CH16012, NASPO ValuePoint Master Agreement for Cloud Solutions.

March 10, 2016

Dear Mr. Hughes,
VMware appreciates the opportunity to respond to the NASPO ValuePoint Cloud Services solicitation through the State of Utah Division of Purchasing. VMware provides the following responses to the requirements of the RFP:

(5.2.1) After review and consideration of the subject RFP, including Attachment A, NASPO ValuePoint Master Agreement Terms and Conditions and Attachment D, Scope of Services, VMware accepts and is willing to comply with the requirements of the RFP and exhibits, as negotiated and finally awarded in a Master Agreement and executed by both parties. VMware recognizes and agrees that it may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

(5.2.2) VMware is responding to this Cloud Services RFP as a direct, prime contract holder and utilized a core team of full time employees to prepare its response. No additional firms or individuals are responsible for writing VMware's proposal response.

(5.2.3) At the time of this proposal submission, VMware affirms it is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs. We maintain an active SAM.gov registration which supports this statement.

(5.2.4) VMware acknowledges that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.

(5.2.5) VMware's proposal for cloud solutions includes the service models SaaS and IaaS which can be deployed through a private, public, hybrid or community cloud. VMware is ready and capable of providing these service and deployment models in accordance with the terms of the subject RFP and resulting Master Agreement.

(5.2.6) VMware's proposal for cloud solutions includes the service models SaaS and IaaS which can be deployed through a private, public, hybrid or community cloud, as explained in more detail in this proposal response, section 6.1. VMware is ready and capable of providing these service and deployment models in accordance with the terms of the subject RFP and resulting Master Agreement. VMware has reviewed the data risk categories provided in the RFP, Attachment D. VMware products are capable of storing and securing data that is classified as low, moderate or high risk data. VMware's product offering aligns with these defined categorizations and is explained in more detail in this proposal response, section 6.1.

We look forward to discussing our proposed response for cloud solutions with you further. Should you have questions or need additional information, please feel free to contact:

Karin Whitwood, Contracts Manager
kwhitwood@vmware.com
571-375-3481

Mark Slafka, Capture Manager
slafkam@vmware.com
703-483-1416

Sincerely,

Digitally signed by Luis A. Mata
DN: cn=Luis A. Mata, o=VMware, ou=Legal, email=lmata@vmware.com, c=US
Date: 2016.03.07 10:46:09 -08'00'

on behalf of
Michael Quinn
Director, Americas Deal Desk
VMware, Inc.
650-427-7679 (office)
916-769-7494 (mobile)
quinnm@vmware.com

Acknowledgement of Amendments {5.3}

ACKNOWLEDGEMENT OF AMENDMENTS TO RFP (SOLICITATION CH16012)

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the final RFP document posted on February 10, 2016.

By signing below, the Offeror attest to reviewing the documents listed above.

VMware, Inc.
Offeror

Digitally signed by Luis A. Mata
DN: cn=Luis A. Mata, o=VMware, ou=Legal, email=lmata@vmware.com, c=US
Date: 2016.03.03 11:05:02 -08'00'

Representative Signature on behalf of Michael Quinn

Amendments to Solicitation CH16012:

- Addendum 1 (Dec 22, 2015)- New Document: Attachment H provided
- Addendum 2 (Dec 24, 2015)- New Document: Solicitation revised to include Vermont's Terms and Conditions
- Addendum 3 (Jan 05, 2016)- New Documents: Documents added as separate documents:
  - Exhibit 1 to Attachment B – CAIQ v3.0.1-09-16-2014;
  - Exhibit 2 to Attachment B – CSA_CCM_v3.0.1-09-16-2014
- Addendum 4 (Jan 12, 2016)- New Document: Contract signature page has been uploaded as "Vendor Info Form" Please complete this document, sign it, and attach it to your proposal.
- Addendum 5 (Jan 15, 2016)- New Documents:
  - Louisiana – has provided its Intent to Participate
  - Virginia – has revised its Intent to Participate which includes Virginia's terms and conditions
- Addendum 6 (Jan 28, 2016)- Description/Bid Comments: Alabama provided its Intent to Participate
- Addendum 7 (Feb 01, 2016)- Florida has submitted an Intent to Participate
- Addendum 8 (Feb 03, 2016)- Documents removed and added:
  - Removed Document: Attachment F – Usage Summary Report Sample
  - Removed Document: Attachment G – Cost Proposal
  - Removed Document: CH16012 – Score Sheet
  - Removed Document: Cloud Solutions RFP CH16012
  - Removed Document: Attachment H – Identification of Service Models
  - New Document: Acknowledgement of Amendments to RFP final
  - New Document: Attachment H - Identification of Service Models
  - New Document: Attachment A – NASPO ValuePoint Master Agreement Terms and Conditions final
  - New Document: Attachment G – Cost Proposal
  - New Document: Cloud Solutions RFP CH16012
  - New Document: CH16012 – Score Sheet
- Addendum 9 (Feb 05, 2016)- Documents removed and added:
  - Removed Document: Cloud Solutions RFP CH16012
  - Removed Document: CH16012 – Score Sheet
  - New Document: Cloud Solutions RFP CH16012
  - New Document: CH16012 – Score Sheet
- Addendum 10 (Feb 10, 2016)- Documents removed and added:
  - Removed Document: Acknowledgement of Amendments to RFP final
  - Removed Document: Cloud Solutions RFP CH16012
  - New Document: Acknowledgement of Amendments to RFP final
  - New Document: Cloud Solutions RFP CH16012

Section 2 Executive Summary {5.4}

5.4 (M) EXECUTIVE SUMMARY

Offerors must provide an Executive Summary of its proposal. An Executive Summary should highlight the major features of an Offeror's proposal. Briefly describe the proposal in no more than three (3) pages. The evaluation committee should be able to determine the essence of the proposal by reading the Executive Summary. Any requirements that cannot be met by the Offeror must be included.

VMware Response:

VMware, Inc. is pleased to propose Cloud Solutions for the furtherance of the NASPO ValuePoint Cooperative Purchasing Program and all participating entities. VMware's cloud solutions are a combination of best value features of technical, management, pricing and reduced business risk. VMware has proposed the following menu of solutions:

- **Infrastructure as a Service:** vCloud Air (vCA), vCloud Government Services (vCGS), Horizon Air Desktop as a Service, Private Cloud Enablement software including our vCloud Suite, vRealize Suite for Cloud Management, Horizon Suite for private Desktop as a Service, Virtual SAN, and NSX network virtualization.
- **Software as a Service:** AirWatch, vRealize Air Compliance, and SocialCast
- **Platform as a Service:** VMware is not proposing a PaaS solution

Table 2 below summarizes VMware's Major Features:

Best Value • **Trusted, Proven:** vSphere is deployed extensively through-out all NASPO states (>371,000 VMs). • **Low-risk, two-way migrations:** No labor required to modify VMs for migration in or out of vCloud Air (vCA) • **No learning curve:** Staff leverage existing VMware operations management skills & tools • **Turn-key High Availability and Disaster Recovery:** Simplified DR and Business Continuity • **No lock-in:** Easy vCA exit migration relative to other clouds (i.e. no app mods or data right issues)	**Favorable Pricing** • **Leveraging Existing Investments in VMware:** More than 90,000 vSphere licenses in the 33 named NASPO states; running >371,000 vSphere VMs; provides VMware with compelling business case for favorable pricing • **Maximize Cost Avoidance:** Substantial cost avoidance when deploying vSphere workloads to vCA. Avoid modification/migration labor required by non-VMware clouds. Reduced labor required to recertify/reaccredit secure workloads. • **Maximizing ROI:** VMware includes peripherals (e.g. load balancers and firewalls) at no charge
Information Technology Dept. Benefits • **Efficiency:** Familiarity with VMware technologies, no re-training, minimized workload refactoring • **Scalability:** Ease of migration of 371,000+ workloads • **Collaboration:** AirWatch for secure content management and mobile device management. SocialCast enables internal social networking • **Flexibility:** Migrate in and out, on-demand • **Security:** Network virtualization and security included with vCA providing a Zero-Trust and Micro-Segmentation features	**Sales/Marketing/Support Coverage** • **Large Nationwide Sales & Marketing Workforce:** Ample internal and partner staffs deployed in all NASPO states will provide sales, marketing and administrative support; Provides the State of Utah and NASPO customers continuous pre- and post-sales cloud service experience • **Adherence to NIST:** Facilitates "apples-to-apples" comparison of VMware offerings to those of others

Table 2. VMware Major Features of our Proposal Response

VMware technology is currently deployed across the United States in more than 15,000 state agencies, local governments, and educational entities. Within the states that intend to participate under this contract, customers have more than 90,000 vSphere licenses deployed running more than 370,000 virtual machines (VMs) (see section 4.4 General Information for more details). The VMware technology used in their data centers, is the same technology used in VMware's proposed IaaS cloud services. Therefore, there is no need to rewrite or recode vSphere workloads to migrate to VMware's cloud solutions. The workloads will function the same in the hybrid cloud as they do within their current data center.

Figure 1 below shows the ease the migration of an application off premise, or back on premise. VMware differentiates itself by providing a hybrid platform that: (i) requires no VM conversions, (ii) offers seamless extensible networking, (iii) is optimized for both existing apps and new apps, (iv) has no vendor lock-in, and (v) eliminates the need for staff retraining, as the same technology that is used in vCloud Air is used in their existing data centers.

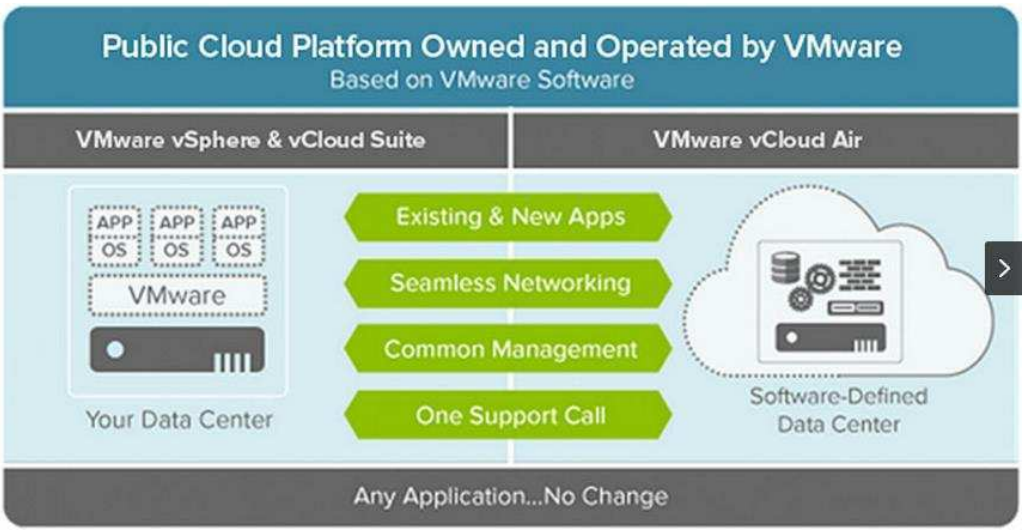


Figure 1. Example of Workload Migration

With the substantial investment that public sector customers have made in VMware, moving an application to vCloud Air can be significantly less costly than with other leading cloud providers. As an example, a customer can move an application to vCloud Air in just a few days. To move that same application to another cloud provider, it could take 30+ days. This is accounting for critical steps such as: database migration; load balancer and firewall migration, training of staff, and comprehensive testing. This time savings can equate to significant cost savings for the customer and help to reduce the possibility of errors with moving the application to the cloud. To put this into context, assume a labor cost of $800 per day. To migrate an application to VMware, the labor cost may equal $4,000 for 5 days compared to more than $26,000 for 30+ days from another cloud provider (see section 4.4 General Information Section for details).

Unlike many of our peers, the vCloud Air solution is the least risky for IT leaders who are not sold on the concept of cloud. With vCloud Air, migrating out of the cloud is as easy as moving into the cloud. If for any reason Participating Entities have a need to move a workload back on-premise, they can simply vMotion their workloads back to their data center or to another cloud provider. Of particular note is the "data-rights" business risk for workload modification that is required to migrate these workloads to a non-VMware cloud solution. Unless the NASPO

customer pays directly for these modifications they will have limited data rights to the modified workload code and therefore data-rights restrictions moving the workload off of the non-VMware cloud solution.

VMware's Cloud strategy is "One Cloud, Any Application, Any Device". This means NASPO customers can build unified hybrid cloud solutions across private, public, and managed clouds. This also includes disaster recovery as a service to provide for continuous operations and geographic High Availability. A unified hybrid cloud lets you rapidly develop, automatically deliver and manage all of your enterprise applications, no matter where they reside, from one, unified platform.

VMware's solutions are leading the way for agencies and organizations to enable a Software-Defined Data Center (SDDC) architecture. SDDC brings together best-in-class virtualized compute, virtualized storage, virtualized networking and management solutions.

The move to cloud computing is an evolution and not all customers are at the same place at a given time. **Figure 2** below depicts the VMware technologies that are applicable to each deployment and delivery model. Whether customers are deploying virtualization technologies within a traditional center, building a private cloud to streamline service offerings, migrating applications to a hybrid or community cloud for excess capacity, or moving to a public cloud for complete outsourcing of operations and management, proposed VMware technologies are the essential to build or enable traditional data centers and private, community, hybrid, and public clouds.

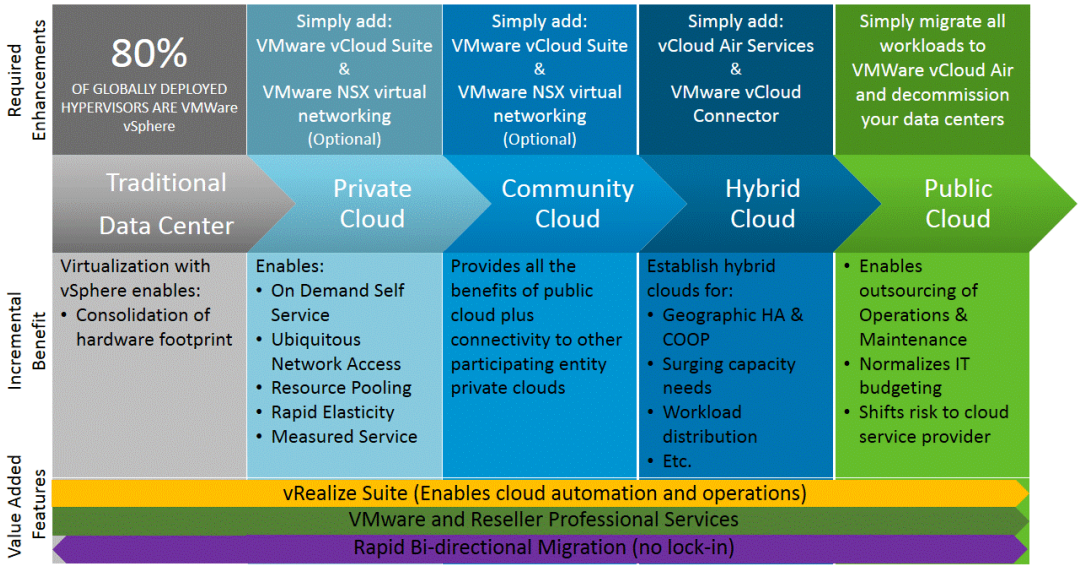


Figure 2. VMware's Support for the Spectrum of Cloud Models.

VMware has more than 15,000 customers across the state agencies, local governments, and educational entities. Combining this extensive customer base, with VMware's Cloud Strategy and SDDC architecture, favorable pricing, cost and risk avoidance, a robust reseller ecosystem, and aggressive sales and marketing strategy, we believe VMware offers a substantial best value to the State of Utah and the NASPO ValuePoint Cloud Contract Participating Entities.

VMware complies with the requirements of RFP and has provided details on how we comply throughout our response. Our proposed exceptions to the terms and conditions may be found in **Appendix A – Exception and/or Additions to the Standard Terms and Conditions.**

Section 3 Mandatory Minimums {5.5}

3.1 GENERAL REQUIREMENTS {5.5} (M)

5.5.1 Offeror must agree that if awarded a contract it will provide a Usage Report Administrator responsible for the quarterly sales reporting described the Master Agreement Terms and Conditions, and if applicable Participating Addendums.

5.5.2 Offeror must provide a statement that it agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading an Offeror's ordering instructions, if awarded a contract.

5.5.3 Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment . Offeror must either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), **Exhibit 1 to Attachment B**, or to submit a report documenting compliance with Cloud Controls Matrix (CCM), **Exhibit 2 to Attachment B**. Offeror must also represent and warrant the accuracy and currency of the information on the completed. Offerors are encouraged to complete and submit both exhibits to Attachment B.

5.5.4 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements. .

(5.5.1) VMware agrees that, if awarded a contract to the cloud solutions RFP (No. CH16012), it will provide a Usage Report Administrator to be responsible for the quarterly sales reporting described in the Master Agreement Terms and Conditions, as finally awarded. VMware understands and affirms that the final form of these reports will be determined after award and reviewed with the awarded Contractors post-award.

(5.5.2) VMware agrees to cooperate with NASPO ValuePoint and SciQuest (and an authorized agent or successor entity to SciQuest). VMware agrees to provide SciQuest with uploading ordering instructions, to facilitate the ordering process by Participating Entities.

(5.5.3) VMware has completed and intends to maintain a completed a Level 1 CSA STAR Registry Self-Assessment which is submitted as a copy under this RFP in **Appendix B**. VMware represents and warrants that, at the time of submission, the accuracy and currency of the information on the completed CSA Star Self-Assessment Form. Please see Exhibit 1 to Attachment B for VMware's submitted CAIQs.

(5.5.4) As part of its proposal must provide a sample of its Service Level Agreements.

Applicable Service Level Agreements (SLA) can be found in **Appendix C.**

5.6 NOT USED

3.2 Recertification of Mandatory Minimums and Technical Specifications {5.7}

5.7 **RECERTIFICATION OF MANDATORY MINIMUMS AND TECHNICAL SPECIFICATIONS**

Offeror must acknowledge that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the technical capabilities discussed in its proposal.

VMware Response:

VMware acknowledges that if awarded a contract, it will annually certify to the Lead State that it meets or exceeds the technical specifications capabilities presented in its proposal.

Section 4 Business Information {6} (M) (E)

4.1 Business Profile {6.1} (M) (E)

Provide a profile of your business including: year started, organizational structure, client base (including any focus by region, market sector, etc.), growth over the last three (3) years, number of employees, employee retention rates (specific for employees that may be associated with the services related to the RFP) over the last two (2) years, etc. **Businesses must demonstrate a minimum of three (3) years of experience providing cloud solutions for large scale projects, including government experience, to be eligible for award. {6.1}**

VMware was founded in 1998 and has grown to become one of the largest software and cloud computing companies in the world. With 2015 revenues of nearly $6.6 Billion, VMware has more than 500,000 customers, 75,000 partners, and 18,000+ employees in 120+ locations around the world. VMware is headquartered in Palo Alto, CA and incorporated in Delaware. VMware's US offices are located in Reston, Virginia; Cambridge, Massachusetts; Atlanta, Georgia; Austin, Texas; San Francisco, California; and Boulder, Colorado.

VMware's Executive Leadership team and area of responsibility is provided below in **Figure 3**.

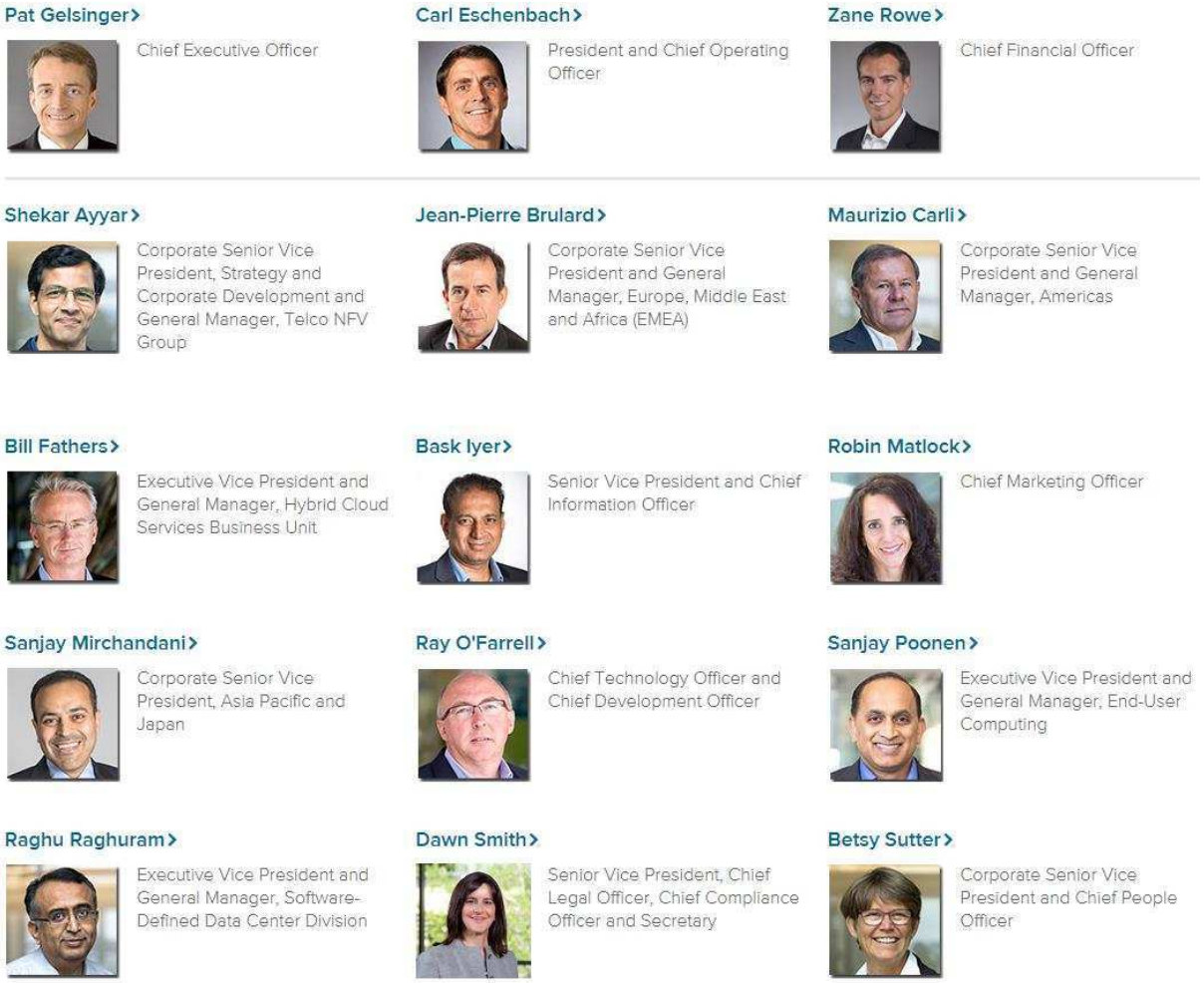


Figure 3. VMware organization structure and executive leadership team

Throughout the states that intend to participate and use this contract, VMware employs more than 4,200 full time employees. **Figure 4** below depicts the number of VMware employees

across the states that intend to use the contract. Within the VMware Public Sector Organization, approximately 10% of those employees will be involved with this contract. They will be providing support and resources for contract management, sales, reseller enablement, engineering, cloud services specialists, professional services, and numerous support roles.

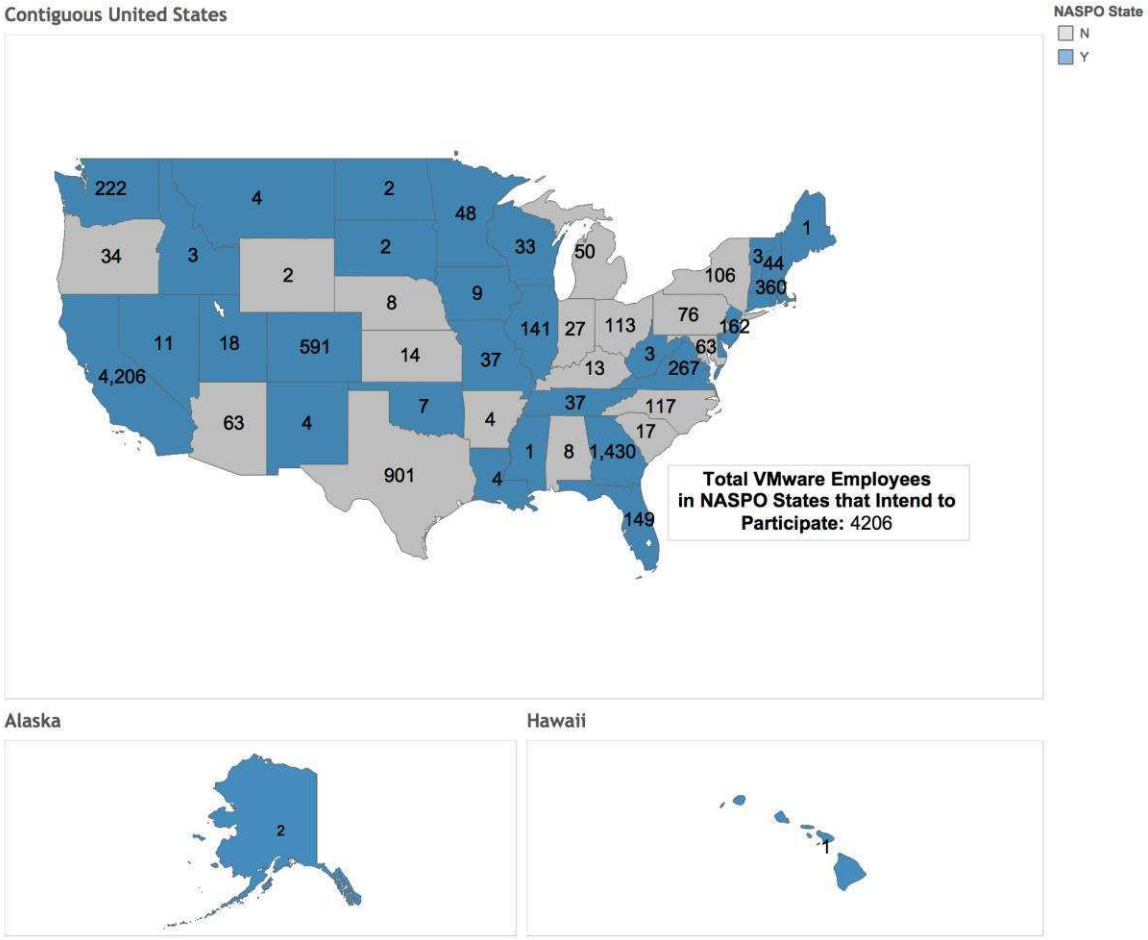


Figure 4. VMware's National Footprint

More than 500,000 customers — including 100% of the Fortune 100 — trust VMware as their virtualization infrastructure platform. VMware works with customers in every industry across the globe. Within the public sector, VMware has more than 15,000 state agencies, local governments, and educational entities as customers.

VMware continues to expand its footprint as we grow our business globally. Historical sales and growth rates for the last three years are provided in the **Table 3** below.

Year (1/1 - 12/31)	Total Annual Revenue ($Billion)	Growth % (Year over Year)
2013	$5.207B	13%
2014	$6.035B	16%
2015	$6.57B	9%

Table 3. VMware Growth Rates

VMware's employee retention rate for 2014 – 2015 is depicted in **Table 4** below:

Year	Retention Rate
2014	86.3%
2015	86.7%

Table 4. VMware Retention Rate

VMware has significant experience helping government customers and educational entities on large scale projects. Provided below are a few examples of projects that VMware led for government and education customers.

1. State of Washington, Department of Information Services – Build Out of VMware Based Private Cloud

The State of Washington Department of Information Services (DIS) contracted with VMware Professional Services to assist with the design and build out of an IaaS Private Cloud. VMware led the planning, requirements gathering, use cases for a prototype implementation, architectural design, build out, and training efforts for DIS staff for their private cloud.

The original value of the contract was more than $625,000. This project started in 2010 and the initial implementation was completed in 2011 and enhancements continue through today. VMware delivered to DIS their private cloud and the scope of services continue to expand based on the agency needs.

2. New York City, Department of Information Technology & Telecommunications

The New York City Department of Information Technology & Telecommunications (DoITT) provides IT services, infrastructure, and telecommunications to New York City's residents, businesses, and visitors. DoITT serves a vast network of 120 agencies, boards, and offices, more than 8,000,000 residents, 300,000 employees, and 230,000 businesses every day- and approximately 50 million visitors each year.

DoITT was faced with multiple agencies requesting infrastructure for applications and test and development platforms. They found it difficult to be responsive to meet demands from agencies and they lacked a common platform or architecture across agencies.

DoITT implemented a self-serve cloud offering based on VMware vCloud Suite. The solution provides a containerized IaaS offering that can be customized to meet agency specific needs. This allows agencies to receive faster provisioning timeframes, provides a significant reduction in physical space in data center, cost avoidance for acquisition cost of infrastructure, and offers business continuity with a disaster recovery solution.

The total value of the project exceed $8M and the implementation began in 2014 and continues today. In addition to this project, VMware has been working with DoITT for more than a decade on IT projects and initiatives to modernize their data center.

3. Columbia University, Development of a Private Cloud with VMware Products and Professional Services

Columbia would wanted to implement automated delivery of workloads to assist in accelerating the infrastructure deployment lifecycle and increase standardization. Columbia partnered with VMware to develop a modernized IT infrastructure that implemented automation and state-of-

the-art tools from the VMware vCloud Suite product set. The engagement served as a launching point for Columbia's long-term strategy to build a stable, manageable internal private cloud with self-service provisioning capability. Columbia's desire is to move from their current fixed IT infrastructure to an elastic cloud with the ability for dynamic scaling of their computing resources. The solution will allow the Columbia internal IT department to become more service-oriented and to deliver services with the agility required by Columbia departments and staff, who are requesting stable, modernized services.

Results Columbia was able to achieve include:

- A standardized monitoring platform to enable real-time analysis and management of the virtual environment.
- A baseline compliance policy that demonstrates the ability to automate the compliance of virtual machines to a standardized configuration.
- A baseline security architecture that allows for agility in the virtual environment while still maintaining the security policies of Columbia University.
- A self-service infrastructure broker with the ability to demonstrate automated deployment of core infrastructure apps.
- This project was initiated in the middle of 2014 through 2015 and had an approximate value of $500,000.

4.2 SCOPE OF EXPERIENCE {6.2} (M)(E)

Describe in detail the business' experience with government or large consortium contracts similar to the Master Agreements sought through this RFP. Provide the approximate dollar value of the business' five (5) largest contracts in the last two (2) years, under which the Offeror provided Solutions identical or very similar to those required by this RFP. Government experience is preferred. {6.2}

VMware Response:

VMware products are offered on numerous procurement vehicles and pricing schedules throughout the public sector. We have experience supporting these contracts that are predominantly held by our distributors and resellers.

The top five government contracts for VMware products are provided in the **Table 5** below. All of the contracts listed are either convenience contracts or have a convenience contract component. The scope of the contracts includes cloud services or cloud enablement technologies. For each contract, there are numerous VMware resellers that facilitate the sales and ordering process through the master contract.

Contract Name	Approximate Annual Sales	Period of Performance
Department of Defense ESI BPA Contract # W91QUZ-09-A-0003	$100M	3/26/2009 – 12/19/2016
Federal GSA Schedule 70 No. GS-35F-0119Y	$72M	12/20/2011 – 12/19/2016
California Software Licensing Program	$15M	07/14/2014 – 07/31/2017
New York, Office of General Services, Misc. Software Contract	$9M	7/15/2010 – 6/14/2016
U. S. Army - Enterprise License Agreement | Blanket Purchase Agreement for VMware	$7M	10/1/2013 – 7/10/2018

Table 5. VMware Procurement Vehicles

On an annual basis, public sector customers (Federal, State, Local, and Education) purchase more than $500M of VMware products and services through a variety of procurement vehicles. VMware sales executives and system engineers have deep experience working with customers on a multitude of opportunities. Their experience includes creating large enterprise wide agreements, architecting complex opportunities that span multiple technologies, and developing blueprints for implementing software defined data centers based on our technologies. Our sales executives and engineers also work in conjunction with our resellers and systems integrators to develop and deliver VMware solutions to best meet the customer objectives.

VMware continues to evolve its portfolio of procurement vehicles across the United States. We are actively pursuing more contracts as a direct prime contract holder. We intend to name multiple resellers to sell our products through our contracts. This approach gives customer's maximum flexibility to select a reseller that best meets their needs for a project. Whether in need of an in-state small / disadvantaged business or national reseller, we aim to offer an array of resellers onto our contract.

We are in active negotiations to be awarded procurement vehicles with: Texas Department of Information Resources, New York Office of General Services, and the Massachusetts Office of Information Technology.

To manage these contracts and more, VMware has built out a public sector contract management team. This team will be focused on the successful management and administration of contracts awarded to VMware.

4.3 FINANCIALS {6.3}(M)

Offeror must provide audited financial statements, of the last two years, to the State that demonstrate that an Offeror meets at a minimum Dun and Bradstreet (D&B) credit rating of 3A2 or better, or a recognized equivalent rating. Please provide the Respondent's D&B Number and the composite credit rating. The State reserves the right to verify this information. If a branch or wholly owned subsidiary is bidding on this RFP, please provide the D&B Number and score for the parent company that will be financially responsible for performance of the agreement.

VMware Inc. is a publicly traded company (VMW) and makes its annual reports available via its investor relations website (http://ir.vmware.com/). The financial information requested in the RFP CH16012 is lengthy and can most efficiently be retrieved from this website. Specifically, the 10-K annual and 10-Q quarterly reports can be obtained by going to the SEC Filings link on the right side of the page and then filtering the view for the specific filing report required, such as annual, quarterly, current reports. VMware is confident that our financial circumstances are stable and provide adequate resources to fulfil the requirements of the contract contemplated. VMware provides the basic, requested financial information in the below **Table 6** and is happy to respond to specific inquiries from the Lead State and Participating Entities, to affirm our financial stability in providing the solutions offered in our proposal response.

Company Name	D&B Number	Composite Credit Rating
VMware, Inc. (Offeror)	048870740	5A3
EMC Corporation (Parent Company)	097447148	5A2

Table 6. VMware Requested Basic Financial Information

VMware's financial strength rating (5A) demonstrates net worth of 60+ million dollars which exceeds the RFP requirement of 3A, or 12-25 million dollars. As provided in VMware's Q4 2015 earnings release, VMware's annual GAAP total revenues were $6.57 billion, up 9% year-over-year or 12% on a constant currency basis. VMware is dedicated to strong financial performance as a competitive, publicly traded company with a responsibility to provide positive returns for its shareholders.

At this time, VMware's risk indicator rating is currently at a "3" indicating "fair condition" which is a rating assigned to concerns believed to be financially sound but with a history of some losses or working capital deficit. The associated risk identified here is for a potential creditor and not for a potential customer and as such, in VMware's opinion, does not pose a financial risk to Utah, NASPO or Participating Entities who may conduct business with VMware. During Q2 2015, VMware reached an agreement with the U.S. Department of Justice ("DOJ") and the General Services Administration ("GSA") to resolve allegations that its sales practices between 2006 and 2013 had violated the federal False Claims Act. The settlement amount was $76 million and was recorded as a reduction of total revenues. VMware considers this activity be a singular incident due to the nature of the claims underlying the matter and measures taken to prevent such concerns in the future. VMware is sensitive to its credit rating and takes its financial responsibility to its shareholders seriously. VMware has committed time and resources to consistently review its business practices to identify and monitor areas of improvement. VMware's business practices continue to develop and mature as the company evolves, with a focus on compliance and process improvement.

4.4 GENERAL INFORMATION {6.4} (E)

4.4.1 Provide any pertinent general information about the depth and breadth of your Solutions and their overall use and acceptance in the cloud marketplace. {6.4.1}

Significant Market Share

Across the 33 states that have expressed interest to use this contract, VMware has more than 90,000 of vSphere licenses deployed today to enable more than 370,000 virtual machines. As we described in the executive summary, VMware vSphere is at the core of cloud computing. **Figure 5** below shows the total number of VMware Virtual Machines deployed by state (for state agencies, local governments, and educational entities).

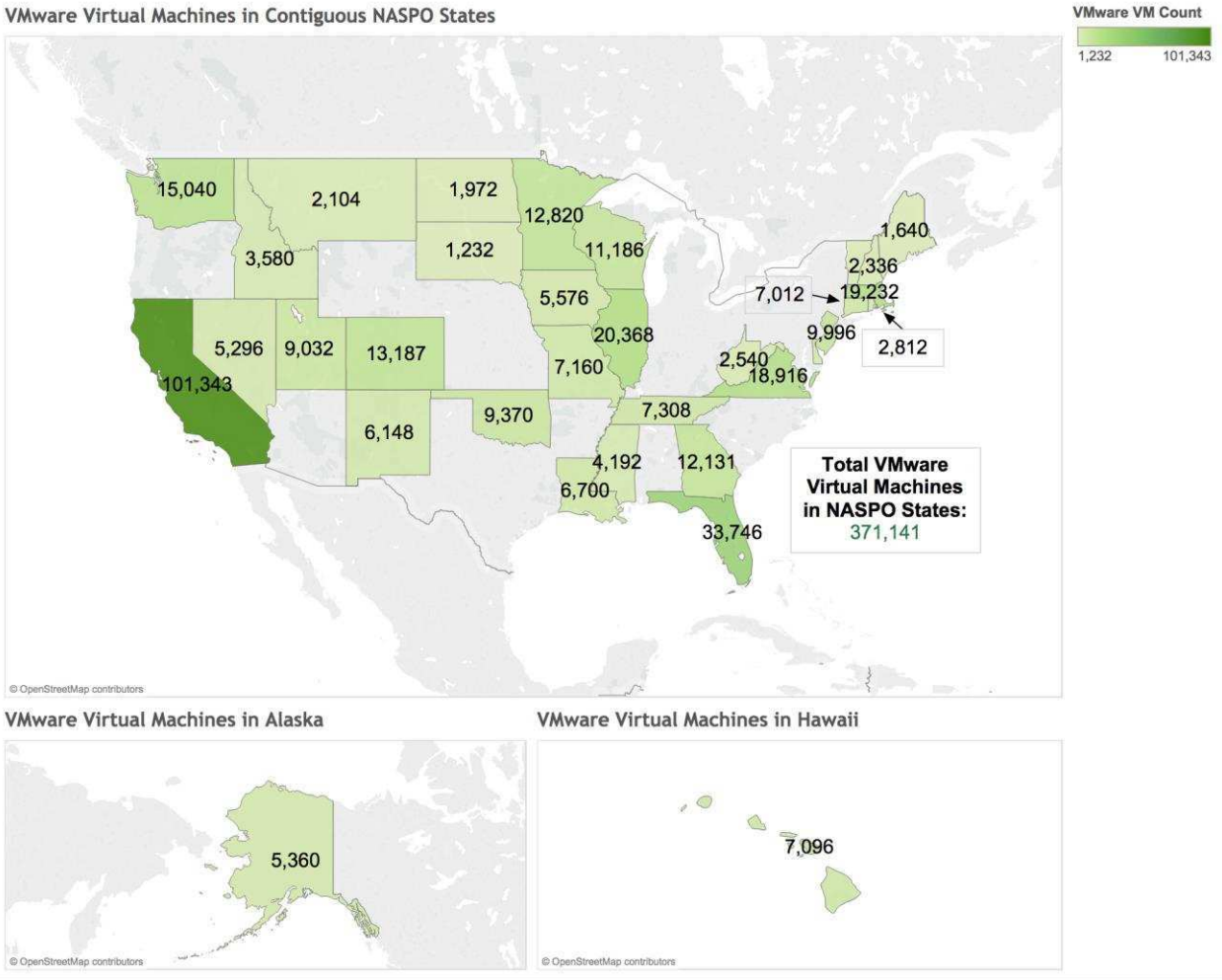


Figure 5. VMware Virtual Machines deployed by State

VMware determined the number of virtual machines using the following calculations. First, we used the actual number of VMware licenses that were currently deployed by NASPO state in 2013, 2014, and 2015. To determine the number of physical servers that are in use, we assumed that 40% of the licenses were running on quad CPU servers and the other 60% were running on dual CPU servers. Next, we assumed that there were 10 virtual machines running on each server to calculate the total virtual machines. **Table 7** shows the calculations that we used to extrapolate the 90,000 vSphere licenses to equate to more than 370,000 virtual machines.

	VMware vSphere Licenses Deployed				Total Lic per 4 Way (Assume 40%)	Total Lic per 2 Way (Assume 60%)	Total Number of 4 way Physical Servers	Total Number of 2 way Physical Servers	WorkLoads (VMs) per Physical Server	Total # of Workloads (VMs) for 4 Way Server	Total # of Workloads (VMs) for 2 Way Server	Total # of Workloads (VMs)
State	2013	2014	2015	Grand Total								
AK	439	589	312	1,340	536	804	134	402	10	1,340	4,020	5,360
CA	7,906	9,149	8,280	25,335	10,134	15,201	2,534	7,601	10	25,336	76,007	101,343
CO	1,562	1,054	681	3,297	1,319	1,978	330	989	10	3,297	9,890	13,187
CT	523	591	639	1,753	701	1,052	175	526	10	1,753	5,259	7,012
DE	277	147	425	849	340	509	85	255	10	849	2,547	3,396
FL	2,723	3,013	2,611	8,347	3,375	5,062	844	2,531	10	8,437	25,310	33,746
GA	982	923	1,127	3,032	1,213	1,820	303	910	10	3,033	9,098	12,131
HI	361	901	512	1,774	710	1,064	177	532	10	1,774	5,322	7,096
IA	573	507	314	1,394	558	836	139	418	10	1,394	4,182	5,576
ID	305	323	267	895	358	537	90	269	10	895	2,685	3,580
IL	1,543	1,995	1,554	5,092	2,037	3,055	509	1,528	10	5,092	15,276	20,368
LA	459	450	766	1,675	670	1,005	168	503	10	1,675	5,025	6,700
MA	1,865	1,682	1,261	4,808	1,923	2,885	481	1,442	10	4,808	14,424	19,232
ME	167	133	110	410	164	246	41	123	10	410	1,230	1,640
MN	1,231	1,084	890	3,205	1,282	1,923	321	962	10	3,205	9,615	12,820
MO	604	673	513	1,790	716	1,074	179	537	10	1,790	5,370	7,160
MS	440	354	254	1,048	419	629	105	314	10	1,048	3,144	4,192
MT	161	238	127	526	210	316	53	158	10	526	1,578	2,104
ND	203	146	144	493	197	296	49	148	10	493	1,479	1,972
NH	184	262	138	584	234	350	58	175	10	584	1,752	2,336
NJ	771	1,078	650	2,499	1,000	1,499	250	750	10	2,499	7,497	9,996
NM	513	485	539	1,537	615	922	154	461	10	1,537	4,611	6,148
NV	386	382	556	1,324	530	794	132	397	10	1,324	3,972	5,296
OK	885	849	609	2,343	937	1,406	234	703	10	2,343	7,028	9,370
RI	159	334	210	703	281	422	70	211	10	703	2,109	2,812
SD	130	28	150	308	123	185	31	92	10	308	924	1,232
TN	593	601	633	1,827	731	1,096	183	548	10	1,827	5,481	7,308
UT	327	399	1,532	2,258	903	1,355	226	677	10	2,258	6,774	9,032
VA	1,540	1,867	1,323	4,730	1,892	2,837	473	1,419	10	4,729	14,187	18,916
VT	187	73	68	328	131	197	33	98	10	328	984	1,312
WA	1,119	1,516	1,125	3,760	1,504	2,256	376	1,128	10	3,760	11,280	15,040
WI	1,012	820	965	2,797	1,119	1,678	280	839	10	2,797	8,390	11,186
WV	302	189	144	635	254	381	64	191	10	635	1,905	2,540
Grand Total	**32,445**	**34,849**	**31,444**	**92,696**								**371,141**

Table 7. Calculation of VMware Virtual Machines deployed by State

Lower Cost of Migration

As highlighted in the executive summary in section 2, moving an application to VMware IaaS services can be significantly less than with other leading cloud providers. As an example, a customer can move an application to vCloud Air in just a few days. To move that same application to another cloud provider it could take 30 days or more. **Table 8** below highlights the typical steps that a customer will need to complete in order to migrate an application to the cloud. We view this cost savings as a significant benefit to customers moving applications to the cloud.

Migration Step	VMware vCloud Air/vCGS	Non-VMware-based Cloud Providers
Obtain training on new cloud technologies	Not necessary	5-10 days
Build a lab environment to validate cloud capabilities	Not necessary	1-3 days
Run test to confirm software is compatible with cloud environment	Not necessary	1-3 days
Research and decide which new proprietary cloud storage technology best suits your application (e.g. block, object, virtual tape, etc.)	Not necessary	.5 days
Convert virtual machines to new format for compatibility with new cloud provider	Not necessary	1-5 days
Import machines into cloud environment	1-5 days	1-5 days
Migrate commercial relational databases to proprietary cloud databases	Not necessary	1-5 days

Migrate load balancers, firewalls, and other peripherals to proprietary cloud equivalents and update applications networking accordingly	Not necessary	1-5 days
Establish security policies and role based access control	1-3 days	1-3 days
Estimated Total Days	5	33
Estimated Cost / Day	$800	$800
Estimated Total Migration Cost	**$4,000**	**$26,400**

Table 8. Estimated costs of migrating an application to VMware vs. another cloud service provider

Industry Recognition

Industry analysts, such as Gartner, have also weighed in on VMware's strengths and market position. In a recent vendor rating report on VMware that was published by Gartner on December 23, 2015, they highlight that "VMware continues to have dominant x86 virtualization market share with a presence in 80% of data centers today". VMware has also been recognized on Gartner's May 2015 Magic Quadrant for Cloud Infrastructure as a Service as one of the "Visionaries" as shown in **Figure 6.**

Figure 6. VMware noted by Gartner as a Visionary in Cloud Services

VMware AirWatch was recognized as a "Leader" on Gartner's June 2015Maqic Quadrant for Enterprise Mobility Management Suites as shown in **Figure 7**.

Figure 7. VMware AirWatch noted by Gartner as a Leader in Enterprise Mobility Management

The significance of this recognition demonstrates VMware's strength in the market, ability to execute well, and vision to change the market. This is further demonstrated by our ease of migration both into and out of cloud and great flexibility that we can offer to customers.

Portable Licensing Unit

VMware recently launched a Portable Licensing Unit (PLU) for vRealize Suite that provides flexibility to deploy the same vRealize Suite license across hybrid and heterogeneous environments such as vSphere-based virtualized environment, third-party hypervisors, physical servers, vCloud Air, and all other supported public clouds. PLU combines the benefits of managing unlimited Operating System Instances (OSIs) / Virtual Machines (VMs) on one vSphere CPU or up to 15 OSIs on a supported public cloud using the same license key.

The PLU metric switches automatically when the workload being managed by vRealize Suite moves from one environment to another. This is a default functionality in vRealize Suite requiring no license conversion and no additional cost, resulting in time and cost savings to end users. The PLU capability is available to all vRealize Suite and vCloud Suite customers – this includes existing customers (on active SnS) and new customers.

Look to the Future

VMware's One Cloud, Any Application, Any Device is more than a tagline. It means that IT organizations can build a unified hybrid cloud across public, private, and managed clouds. VMware is helping customers implement the Software-Defined Data Center (SDDC) architecture, which brings together compute, storage, networking virtualization and management offerings. The NASPO Cloud Services Contract is the enabler to allow customers to purchase the SDDC components to implement into their environment.

VMware has more than 15,000 customers today across state agencies, local governments, and educational entities. Combining this extensive customer base, with the SDDC architecture and strategy, enterprise class and award winning products, a robust partner ecosystem, and aggressive sales and marketing strategy, we believe VMware offers a valuable and in demand product offering for the NASPO ValuePoint Cloud Contract and Participating Entities.

4.4.2 Offeror must describe whether or not its auditing capabilities and reports are consistent with SAS 70 or later versions including, SSAE 16 6/2011, or greater. {6.4.2}

VMware Response:

Yes. VMware's auditing capabilities and reports meet or exceed this requirement. VMware vCloud Air has achieved ISO/ IEC 27001:2005 Certification of its Information Security Management System and has completed SOC II Type 1, SSAE 16 SOC 1 Type II and SOC 2 Type II examinations.

4.5 BILLING AND PRICING PRACTICES{6.5}(E)

DO NOT INCLUDE YOUR PRICING CATALOG, as part of your response to this question.

4.5.1 Describe your billing and pricing practices, including how your billing practices are transparent and easy to understand for Purchasing Entity's. {6.5.1}

VMware Response:

Pricing Practices

VMware sells our products from a published global price list and price quotes show a detailed breakdown of the service that was ordered with a description of the characteristics of the offer. Our business model was designed to allow customers to purchase our products from authorized resellers or partners. Our partners work directly with end customers on the design of VMware solutions, create the necessary bill of material for items they wish to purchase, manage the invoice and payment process directly with the end customer, and can provide professional or installation services for the products purchased. Our customers are very familiar and comfortable with this process.

When placing an order for VMware products, currently the customer can submit their purchase order to the authorized reseller of their choice for processing and fulfilment. Under the NASPO cloud services contract, this step would be completed through the eMarketplace according to the ordering instructions that VMware will provide to SciQuest. At the time of placing the order, the authorized reseller may then offer additional discounts as needed, based upon the scope, size and competition of the order, (i.e. additional discounts on the minimum discount offered under the master contract).

Additionally, VMware may agree to process an order directly without the use of an authorized reseller. If the customer prefers this option, they can submit their purchase order directly to VMware for processing, as will also be defined in the ordering instructions provided to SciQuest.

All of VMware's products are listed on our published price lists. For each product we sell, customers can see the specific part number, a brief description of the product or service and the list price for the item. For all products offered under this contemplated contract, the price lists will be posted on the VMware NASPO Cloud Contract webpage and users can access these files for their reference.

Billing Practices

When a customer orders a cloud service from VMware, they will have the option to select the subscription term or length of service. VMware offers 1, 12, 24, or 36 month lengths of service. If selecting a 1 month subscription term, the payment would also be for 1 month. The customer can continue to order and pay for the service on a month to month basis. If a customer selects a 12, 24, or 36 month subscription term, they prepay for the term selected. The prepayment provides the customer with a lower total price due to the extended subscription term for which they are committing.

Provided below is a sample customer invoice **Figure 8**. The invoice clearly outlines the customer and billing information and the services that the customer purchased in an easy to read format. Within the invoice, the customer is able to see the product part number ordered, description of the product, subscription term of service, and pricing information.

vmware

Invoice

VMware, Inc.
3401 Hillview Ave
Palo Alto CA 94304
United States
Phone # 650 427 5000
Fax # 650 644 0376
Email ar@vmware.com

Invoice #	Invoice Date	Payment Terms
[redacted]	[redacted]	NET 30
Sales Order #	**Customer PO #**	**Due Date**
[redacted]	[redacted]	[redacted]
Billing Period	**Page**	**Federal Tax Id #**
20-DEC-2013 to 19-DEC-2015	1 of 1	[redacted]

Bill To :
[redacted]

Remit To: By Check
VMware, Inc.
Dept. CH10806
Palatine, IL 60055-0806

Ship To :
[redacted]

Remit To: By Bank Wire
VMware, Inc.
[redacted]

Customer #	Location	Entitlement Account
[redacted]	[redacted]	[redacted]

Line	SID	Part Number	Description	Date	Qty	Unit Price	Amount
1	[redacted]	HSV-A3ACR-24PT0-C1S	VMware vCloud Hybrid Service - Virtual Private Cloud A3A - Core Subscription - 24 Month Prepaid	20-DEC-13 to 19-DEC-15	1	[redacted]	[redacted]
2	[redacted]	HSV-A3ASP-24PT1-C1S	VMware vCloud Hybrid Service - Virtual Private Cloud A3A - Production Support Sub - 24 Month Prepaid - Tier 1	20-DEC-13 to 19-DEC-15	1	[redacted]	[redacted]
3	[redacted]	HSV-A3ACP-24PT1-C1S	VMware vCloud Hybrid Service - Virtual Private Cloud A3A - Compute Subscription - 24 Month Prepaid - Tier 1	20-DEC-13 to 19-DEC-15	1	[redacted]	[redacted]
4	[redacted]	HSV-A3AIP-24PT0-C1S	VMware vCloud Hybrid Service - Virtual Private Cloud A3A - Public IP Addresses Subscription - 24 Month Prepaid	20-DEC-13 to 19-DEC-15	1	[redacted]	[redacted]
5	[redacted]	HSV-A3AST-24PT1-C1S	VMware vCloud Hybrid Service - Virtual Private Cloud A3A - Primary Storage Subscription - 24 Month Prepaid - Tier 1	20-DEC-13 to 19-DEC-15	1	[redacted]	[redacted]
6	[redacted]	HSV-A3ABW-24PT0-C1S	VMware vCloud Hybrid Service - Virtual Private Cloud A3A - Internet Bandwidth Subscription - 24 Month Prepaid	20-DEC-13 to 19-DEC-15	1	[redacted]	[redacted]

Comments:

Sub Total : [redacted]
Sales Tax :
Total : USD

* This invoice incorporates and is subject to VMware's standard invoice terms and conditions, available at http://www.vmware.com/pdf/invoice_terms.pdf *

Figure 8. Sample VMware invoice to a customer.

4.5.2 Identify any typical cost impacts that a Purchasing Entity might need to consider, if any, to implement your cloud solutions. {6.5.2}

Other than the cost to purchase the VMware cloud service as identified and described in the price list, customers could potentially have zero additional costs. This is possible because moving to VMware cloud services is easy when already running VMware vSphere on premise. The VMware technology used on premise is the same technology used for our IaaS cloud offerings. Therefore, there is no need to rewrite or recode the application. vCloud Air already supports the 5,000+ applications and 90+ operating systems certified for vSphere. The application will behave the same in the hybrid cloud as it does within its current data center. This saves time and money because there is no VM conversions, no vendor lock-in, and the staff that operates the on premise data center is using the same technology to run the data center in vCloud Air.

Alternatively, there are two potential additional costs that customers may need to consider when using vCloud Air are:

- **Software vendor licensing –** Example: Microsoft will charge a cloud tax for any Microsoft licenses used in vCloud Air Virtual Private Cloud. If a customer chooses our Dedicated Cloud then there are no charges from the software vendors.
- **Network connections** – For some workloads migrated to vCloud Air, a customer may decide to provision their own dedicated circuits to vCloud Air. Those charges would be the customer's responsibility.

If a customer is not using VMware technology today to virtualize their data center infrastructure, they would first need to purchase VMware vSphere. Once virtualized on their technology they can seamlessly migrate their workloads to our cloud.

A positive cost impact the customer may wish to consider is selecting a longer subscription term of service (i.e. 24 or 36 months). VMware offers more favorable pricing for the prepaid commitment for these longer subscription service terms.

4.5.3 Offeror must describe how its Solutions are NIST compliant, as defined in NIST Special Publication 800-145, with the service models it offers. {6.5.3}

VMware Response:

An extensive and detailed explanation of the ways in which VMware's proposed offerings are compliant with NIST Special Publication 800-145 is provided in section 6.1 below.

4.6 SCOPE AND VARIETY OF CLOUD SOLUTIONS {6.6}(E)

Specify the scope and variety of the Solutions you offer under this solicitation. You may provide a list of the different SaaS, IaaS, and/or PaaS services and deployment models that you offer

VMware Response:

Please refer to Section 6.1.3.a – 6.1.3.c of our response for a complete listing of the VMware's IaaS, SaaS, and IaaS Private Cloud Enablement solutions.

4.7 BEST PRACTICES {6.7} (E)

Specify your policies and procedures in ensuring visibility, compliance, data security and threat protection for cloud-delivered services; include any implementations of encryption or tokenization to control access to sensitive data.

VMware Response:

VMware follows and maintains documented internal policies and procedures for ensuring visibility, compliance, data security, and threat protection.

As evidence of this, VMware has obtained the following industry and Government certifications which require that we utilize and maintain these policies and procedures. These certifications include audit and/or accreditation of our high-quality auditable policies and procedures in the categories requested above as a minimum mandatory requirement. **Table 9 and 10** below lists specific certifications.

vCloud Air Compliance Certifications:

Certification / Attestation	Summary
ISO 27001:2005 **Demonstrates:** • *Visibility* • *Compliance* • *Data Security* • *Threat Protection*	ISO/IEC 27001:2005 formally specifies an information security management system (ISMS) to bring information security under explicit management control. VMware was formally audited and is certified compliant with the ISO/IEC 27001:2005 standard. We keep an ISO/IEC 27001 audited and certified policies and procedures including: • An Organizational Security Policy, • Statement of Applicability (SOA), • and Risk Treatment Plan. As required by ISO/IEC 27001:2005, VMware has a security management body that meets regularly to oversee our information security management system and to confirm that these policies and procedures are being followed. We are under go annual follow-up ISO 27001:2005 reviews to confirm that our ISMS continues to operate as specified and intended.
SOC 1 Type II (SSAE 16) **Demonstrates:** • *Visibility* • *Compliance*	SOC 1 is relevant to the visibility and compliance aspects of this NASPO requirement. SOC 1 is a report on controls at a Service Organization which are relevant to its client's internal control over financial reporting and can assist the client's financial auditors with laws and regulations such as the Sarbanes–Oxley Act. SOC 1 Type II is a report on policies and procedures placed in operation and tests of operating effectiveness for a period of time. SSAE 16 type II reports include the examination and confirmation steps involved in a type I examination plus an evaluation of the operating effectiveness of the controls for a period of at least six consecutive calendar months. SOC 1 enables the auditor to perform risk assessment procedures, and if a Type II report is performed, to assess the risk of material misstatement of financial statement assertions affected by the service organization's processing.
SOC 2 Type 2 **Demonstrates:** • *Visibility* • *Compliance* • *Data Security* • *Threat Protection*	The SOC 2 Type 2 reports on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls. It focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system, as opposed to SOC 1/SSAE 16 which is focused on the financial reporting controls. The Trust Service Principles which SOC 2 is based upon cover four areas: Policies, Communications, Procedures, and Monitoring. Each of the principles have defined criteria (controls) which must be met to demonstrate adherence to the principles and produce an unqualified opinion (no significant exceptions found during the audit). VMware's vCloud Air SOC 2 compliance demonstrates that our services, policies and procedures have been audited to confirm that they provide:

	Security: vCloud Air is protected both logically and physically against unauthorized access. **Availability:** The system is available for operation and use as committed and agreed upon with clients. **Processing Integrity:** vCloud Air system processing is complete, accurate, timely and authorized. **Confidentiality:** Information that is designated "confidential" is protected as committed or agreed upon with clients. **Privacy:** vCloud Air conforms with VMware's Privacy notice and with privacy principals put forth by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants.
SOC 3 **Demonstrates:** • *Visibility* • *Compliance* • *Data Security* • *Threat Protection*	The Service Organization Control 3 (SOC 3) report outlines information related to a service organization's internal controls for security, availability, processing integrity, confidentiality or privacy. This document includes a service auditor's report on whether the entity maintained effective controls over its system as it relates to the principle being reported on i.e., security, availability, processing integrity, confidentiality, or privacy, based on the applicable trust services criteria.
HIPAA **Demonstrates:** • *Visibility* • *Compliance* • *Data Security* • *Threat Protection*	The Health Insurance Portability and Accountability Act (HIPAA) Privacy regulations require health care providers and organizations, as well as their business associates, develop and follow procedures that ensure the confidentiality and security of protected health information (PHI) when it is transferred, received, handled, or shared. This applies to all forms of PHI, including paper, oral, and electronic, etc. Furthermore, only the minimum health information necessary to conduct business is to be used or shared. VMware offers a Business Associate Agreement (BAA) to all interested customers using our US-based data centers. The BAA was designed in conjunction with a leading law firm with expertise in HIPAA and provides fair and reasonable terms for healthcare providers, insurers, and other organizations. VMware has completed an independent third party examination of vCloud Air against applicable controls of HIPAA.
CSA STAR **Demonstrates:** • *Visibility* • *Compliance* • *Data Security* • *Threat Protection*	The Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR) is an industry program for security assurance in the cloud. STAR encompasses key principles of transparency, rigorous auditing, harmonization of standards, and continuous. STAR certification provides multiple benefits, including indications of best practices and validation of security posture of cloud offerings. STAR consists of three levels of assurance, which currently cover four unique offerings all based upon a succinct yet comprehensive list of cloud-centric control objectives in the CSA's Cloud Controls Matrix (CCM). CCM is the only meta-framework of cloud-specific security controls, mapped to leading standards, best practices and regulations. CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to cloud computing. VMware vCloud Air completed a CSA STAR Registry Self-Assessment CAIQv3.01 and it was published on December 31, 2014. VMware AirWatch has also completed a CAIQv3.0.1 which accompanies our response.
UK G-Cloud 6 Assertation *Demonstrates:* • *Visibility* • *Compliance* • *Data Security* • *Threat Protection*	All suppliers wishing to include their cloud service offerings within the UK Government's Digital Marketplace as a G-Cloud 6 service are now mandated to complete a set of questions regarding security. The questions are based on the UK Government Communications-Electronics Security Group's (CESG) Cloud Security Principles and are aimed at getting consumers of services to assess whether supplier security assertions meet their own particular security needs. VMware is a G-Cloud 6 provider and has provided a G-Cloud 6 Security Attestation demonstrating that our policies and procedures ensure visibility, compliance, data security and threat protection for cloud-delivered services.

Table 9. vCloud Air Certifications

vCloud Government Service:

Certification / Attestation	Summary
FedRAMP **Demonstrates:** • *Visibility* • *Compliance* • *Data Security* • *Threat Protection*	The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP authorized and audits VMware's vCloud Air using its three step process: • **Security Assessment:** The security assessment process uses a standardized set of requirements in accordance with FISMA using a baseline set of NIST 800-53 controls to grant security authorizations. • **Leveraging and Authorization:** Federal agencies view security authorization packages in the FedRAMP repository and leverage the security authorization packages to grant a security authorization at their own agency. • **Ongoing Assessment & Authorization:** Once an authorization is granted, ongoing assessment and authorization activities must be completed to maintain the security authorization. Coalfire completed the independent assessment of the VMware vCloud Government Service (vCGS) under the Federal Risk and Authorization Management Program (FedRAMP), and that the vCGS cloud was granted a provisional authority to operate (P-ATO) from the FedRAMP Joint Authorization Board (JAB).
ITAR **Demonstrates:** • *Compliance* • *Data Security* • *Threat Protection*	VMware vCGS is compliant with the International Traffic in Arms Regulations (ITAR). ITAR controls the export and import of defense-related articles and services on the United States Munitions List (USML). The Department of State Directorate of Defense Trade Controls (DDTC) interprets and enforces ITAR. Its goal is to safeguard U.S. national security and further U.S. foreign policy objectives. For practical purposes, ITAR regulations dictate that information and material pertaining to defense and military related technologies may only be shared with U.S. Persons unless authorization from the Department of State is received or a special exemption is used. U.S. Persons (including organizations) can face heavy fines if they have, without authorization or the use of an exemption, provided foreign persons with access to ITAR-protected defense articles, services or technical data. VMware's ITAR compliance illustrates the extents to which we go to ensure the data security and threat protection for the vCGS service.
FISMA **Demonstrates:** • *Visibility* • *Compliance* • *Data Security* • *Threat Protection*	The Federal Information Security Management Act of 2002 is a United States federal law enacted in 2002. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. VMware vCloud Air is FISMA Moderate Certified. To achieve this level, VMware's processes and procedures were audited with a focus on but not limited to the following: • Risk management • Continuous monitoring • Incident response and reporting • Security training • Plan of actions and milestones • Remote access management • Identity and access management • Configuration management • Contingency planning • Contractor systems • Security capital planning

Table 10. vCGS Certifications

For additional details on VMware certifications, see sections 6.6.1 and 6.6.2 below.

Participating Entities may obtain VMware's vCloud Air and vCloud Government Service policies and procedures for ensuring visibility, compliance, data security and threat protection for its cloud delivered services via their VMware NASPO Contracts Manager after appropriate NDAs are in place.

Access Control and Tokenization

The vCloud Air provides software and functionality to help protect content from unauthorized access such as firewalls, load balancers, IPSec VPNs. You may deploy additional capability to address other security controls such as data encryption, intrusion detection, file integrity monitoring, etc.

VMware vCloud Government Service requires two factor authentication via hardware token.

Section 5 Organization and Staffing {7} (ME)

5.1 Contract Manager {7.1} (ME)

5.1 The Offeror must provide a Contract Manager as the single point of contact for management of the NASPO ValuePoint Master Agreement, administered by the State of Utah. The Contract Manager must have experience managing contracts for cloud solutions.

VMware Response:

VMware proposes Karin Whitwood, as the named Contract Manager to support the NASPO Cloud Solutions Master Agreement and the subsequent Participating Addenda under it. Karin is the single point of contact to a focused, elite team of seasoned professionals who will also be available to support and address the multi-faceted questions and issues VMware expects may arise under this contract vehicle due to the newness and rapidly evolving nature of cloud computing. This team will be accessible to NASPO, Utah Procurement as the Lead State, and all Participating Entities via VMware's single email point of contact, provided below.

5.1.1 Provide the name, phone number, email address, and work hours of the person who will act as Contract Manager if you are awarded a Master Agreement. {7.1.1}

VMware Response:

VMware recognizes the importance and value of the Cloud Solutions contract vehicle and has invested in staff, and is examining its infrastructure and sales teams to be prepared meet the demand of Participating Entities across the U.S. for the cloud services described. To ensure responsiveness and high quality support, VMware's contract management plan includes the following:

Single point of contact Karin Whitwood, Contract Manager, via VMware's NASPO Cloud Solutions dedicated email (NASPO-CloudSolutions@vmware.com), which will be activated post award. This email address will be posted to our VMware –NASPO Cloud Solutions website, which will be established post award and maintained for the term of the Master Agreement with current contact information. Access to support via this email is available 7am Eastern time – 6pm Pacific time, U.S. A response to the email inquiry will be provided within one business day.

Karin Whitwood, Contract Manager
VMware, Inc.
12100 Sunset Hills Road, Suite 600, Reston, VA 20190
Phone: 571-375-3481 (available by phone 8:00am Eastern – 5pm Eastern)
Email: NASPO-CloudSolutions@vmware.com

5.1.2 – 5.1.3 Describe in detail the Contract Manager's experience managing contracts of similar size and scope to the one that will be awarded from this RFP. Provide a detailed resume for the Contract Manager. {7.1.2}

Describe in detail the roles and responsibilities of the Contract Manager as they apply to the NASPO ValuePoint Master Agreement that will be awarded from this RFP.{7.1.3}

VMware Response:

Named Contract Manager: Karin Whitwood. Ms. Whitwood brings over ten years of commercial, federal, state and local contract management experience in IT, consulting, audit, and national security contracts. Karin has successfully managed GSA schedules, State MAS contracts and IDIQ contracts of similar size and scope including, GSA IT70, GSA Alliant, TXMAS, CMAS, TX DIR, WA Department of Enterprise Services Master Agreement, NY OGS Master Agreement, FL DGS Master Agreements, PA COSTARS Cooperative Contracts. Karin is named key personnel and will be responsible for Master Agreement and Participating Addenda negotiations and ongoing contract management to include the additional contractual requirements such as sales and usage reporting. A detailed resume illustrating Karin's experience can be found in **Appendix D Resumes**.

Named Program Manager: Peter Brandano. Mr. Brandano brings 20 years of technical and project management experience in in software and systems engineering and enterprise IT technical and program management. In these areas, Peter has more than five years of technical program management and engineering experience specific to cloud solutions, services, and brokerage programs. Peter has provided exceptional engineering, management, and customer support under contracts of similar size and scope such as the Texas Department of Information Resources (TX DIR) Cloud Services program and the US Marine Corps Enterprise IT Services (MCEITS) Private Cloud program. Peter is named key personnel to the contract management team function to bring specific skills and expertise to the technical and programmatic aspect of contract management. A detailed resume illustrating Peter's experience can be found in **Appendix D Resumes**.

Additional Support Team. VMware employs highly skilled engineers, product specialists, security specialists, programmers, sales and support teams. These team members and their knowledge, skills and abilities are available to Participating Entities via the single point of contact named above. VMware is a leader in cloud solutions and as such, we put our entire team of employees behind our offering.

Section 6 Technical Response {8} (ME)

6.1 TECHNICAL REQUIREMENTS {8.1} (M) (E)

6.1.1 Offeror must identify the cloud service model(s) and deployment model(s) it intends to provide to Eligible Users. See Attachment D. {8.1.1}

VMware Response:

VMware intends to provide **Infrastructure as a Service** (IaaS) in the Public, Private, Hybrid, and Community Cloud deployment models to eligible users. In addition, we are proposing several **Software as a Service** (SaaS) offerings in the Public cloud deployment model to eligible users. At this time, we are not proposing Platform as a Service (PaaS) offerings in any delivery model or SaaS offerings in the Private, Hybrid or Community cloud delivery models. This is because we do not directly own or offer a PaaS offering or Private, Hybrid, or Community SaaS offerings. **Table 11** below summarizes our catalog of offerings.

	Public	Private	Hybrid	Community
IaaS	• vCloud Air • Horizon Air Desktops and Apps	• vCloud Suite • vRealize Suite • NSX • VSAN • AirWatch • Horizon 6	• vCloud Suite and • vCloud Air	• vCloud Suite and vCloud Air
PaaS				
SaaS	• AirWatch • vRealize Air Compliance • Socialcast			

Table 11. Summary VMware NASPO Catalog

The majority of our offerings fall under the IaaS delivery model with the exception of AirWatch, vRealize Air Compliance, and Socialcast, which are SaaS offerings. The cloud services catalog that VMware is proposing is presented in detail in below in sections 6.1.3.a, 6.1.3.b, and 6.1.3c below.

Our Approach to Answering Each Requirement

An individual response is provided to all questions in RFP section 8.1.3 for each of the following groups of products:

- **VMware's Public IaaS Services:** All vCloud Air & vCGS IaaS offerings described in section 6.1.3.a below.
- **VMware's Public SaaS Services:** All AirWatch SaaS offerings and VMware vRealize Air described in section 6.1.3.b below.
- **VMware's Private, Hybrid, and Community IaaS Enablement Offerings:** All products listed in the Private, Hybrid, and Community IaaS Enablement catalog provided in section 6.1.3.c below.

This was done because the services which fall within each group meet the NIST essential characteristic requirements in the same way and are covered by a single response. Where exceptions exist for a particular service or product, an explanation is provided within the answer.

6.1.2 For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the following characteristics, as defined in NIST Special Publication 800-145: {8.1.2.}

VMware Response:

All of the proposed VMware Cloud Services meet the NIST essential characteristics as described in sections 6.1.2.1.a - 6.1.2.5.c below.

6.1.2.1 NIST Characteristic - On-Demand Self-Service: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how self-service technical capability is met. {8.1.2.1}

VMware Response:

The following table explains how each service in the proposed catalog found below in sections 6.1.3.a – 6.1.3.c satisfies the NIST definition of On-demand self-service. **Our responses were provided in the order that the RFP questions were asked. As a result, the following compliance tables discuss products that have not yet been introduced to the reader. Prior to reviewing the compliance tables in this section, the reader may benefit from reviewing of our proposed product catalogs which are provided in the answer to section 6.1.3.a-6.1.3.c.**

6.1.2.1.a On-Demand Self-Service Capabilities of VMware's Public IaaS Services

Table 12 provides proof that VMware's proposed Public IaaS services provide On-Demand Self-Service as defined by NIST. For details on each service discussed below, see VMware's proposed IaaS Catalog in section 6.1.3.a below.

VMware's Private, Hybrid and Community Cloud Offerings	Requirement
Infrastructure as a Service (IaaS)	**Service must meet the following NIST definition of On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
VMware vCloud Air Virtual Private Cloud OnDemand	**Complies.** vCloud Air OnDemand service meets NIST on-demand self-service characteristics. vCloud Air consumers can unilaterally provision compute resources with no human interaction. Customers can consume compute resources by creating an account and building compute workloads paid via credit card requiring no interaction with VMware to facilitate. The vCloud Air Service Offerings include access to two self-service consoles: My VMware Account Management Console ("My VMware") provides access to subscription status, integrating navigation, viewing and management of all VMware product licenses and support under a single account. VMware vCloud Air Console ("Console") is the primary interface for access, consumption, and management of cloud resources purchased from VMware, including virtual data center

	management, configuration of network services, and virtual machine instance lifecycle management. For more advanced management tasks, the Console provides direct access to vCloud Director under the same sign-on. VMware will also provide organization administrator access to the vCloud Application Programming Interface (API) for programmatic resource management or workload migration through VMware vCloud Connector and vCloud Air Hybrid Cloud Manager.
VMware vCloud Air Dedicated Cloud	**Complies.** vCloud Air Dedicated Cloud service meets NIST on-demand self-service characteristics. vCloud Air Dedicated Cloud consumers must initially contact VMware to purchase dedicated service via an enterprise license agreement purchase order, or subscription purchasing program. Once purchased, a user can unilaterally provision compute resources with no human interaction with VMware. As with vCloud Air Virtual Private Cloud On Demand, this offering includes access to the My VMware Account Management Console ("My VMware") and the VMware vCloud Air Console ("Console"). Both are described in detail above. VMware will also provide organization administrator access to the vCloud API.
VMware vCloud Air Virtual Private Cloud	**Complies.** vCloud Air Virtual Private Cloud service meets NIST on-demand self-service characteristics. In addition to the OnDemand offering discussed above, users may pre-purchase vCloud Air Virtual Private Cloud services via an enterprise license agreement purchase order, or subscription purchasing program. Once purchased, a user can unilaterally provision compute resources with no human interaction with VMware. As with vCloud Air Virtual Private Cloud On Demand, this offering includes access to the My VMware Account Management Console ("My VMware") and the VMware vCloud Air Console ("Console"). Both are described in detail above. VMware will also provide organization administrator access to the vCloud Application Programming Interface (API).
VMware vCloud Government Service (vCGS) Dedicated Cloud	**Complies.** vCloud Government Service (vCGS) Dedicated Cloud service meets NIST on-demand self-service characteristics. vCGS Dedicated Cloud consumers must initially contact VMware or an authorized reseller to purchase dedicated service via an enterprise license agreement purchase order, or subscription purchasing program. Once purchased, a user can unilaterally provision compute resources with no human interaction with VMware. As with vCloud Air Virtual Private Cloud On Demand, this offering includes access to the My VMware Account Management Console ("My VMware") and the VMware vCloud Air Console ("Console"). Both are described in detail above. VMware will also provide organization administrator access to the vCloud API.
VMware vCloud Government Service (vCGS) Virtual Private Cloud	**Complies.** vCloud Government Service (vCGS) Virtual Private Cloud service meets NIST on-demand self-service characteristics. vCGS Virtual Private Cloud consumers must initially contact VMware to purchase dedicated service via an enterprise license agreement purchase order, or subscription purchasing program. Once purchased, a user can unilaterally provision compute resources with no human interaction with VMware. As with vCloud Air Virtual Private Cloud On Demand, this offering includes access to the My VMware Account Management Console ("My VMware") and the VMware vCloud Air Console ("Console"). Both are described in detail above. VMware will also provide organization administrator access to the vCloud API.
VMware vCloud Air Disaster Recovery	**Complies.** vCloud Air Virtual Private Cloud service meets NIST on-demand self-service characteristics. In addition to the OnDemand offering discussed above, users may pre-purchase vCloud Air Disaster Recovery Cloud services via an enterprise license agreement purchase order, or subscription purchasing program. Once purchased, a user can unilaterally provision compute resources with no human interaction with VMware. As with vCloud Air Virtual Private Cloud On Demand, this offering includes access to the My VMware Account Management Console ("My VMware") and the VMware vCloud Air Console ("Console"). Both are described in detail above. VMware will also provide organization administrator access to the vCloud API.
VMware vCloud Air Data Protection	**Complies.** A subscription to Data Protection can be purchased through MyVMware. After the subscription is activated, a customer can begin using Data Protection through the vCloud Air console. As with vCloud Air Virtual Private Cloud On Demand, this offering includes access to the My VMware Account Management Console ("My VMware") and the VMware vCloud Air Console

	("Console"). Both are described in detail above. VMware will also provide organization administrator access to the vCloud API.
VMware Continuent	**Complies.** VMware continuant meets NIST on-demand self-service characteristics. User must first purchase VMware continuant software via an enterprise license agreement purchase order, or subscription purchasing program. Once purchased, a user can download and install VMware continuent with no human interaction with VMware.
VMware vCloud Air Block Storage	**Complies.** VMware vCloud Air Block storage is included with the Dedicated, Virtual Private Cloud, and On Demand instances discussed above. At the time of purchase, you can specify which type of storage you would like for your compute solution. As your environment grows or requirements shift, you can simply add more storage and select your storage tier as needed. As with vCloud Air Virtual Private Cloud On Demand, this offering includes access to the My VMware Account Management Console ("My VMware") and the VMware vCloud Air Console ("Console"). Both are described in detail above. VMware will also provide organization administrator access to the vCloud API.
VMware vCloud Air Object Storage	**Complies.** vCloud Air Object Storage service meets NIST on-demand self-service characteristics. vCloud Air consumers can unilaterally provision object storage resources with no human interaction. Customers can consume storage resources by creating an account and building storage workloads paid via credit card requiring no interaction with VMware to facilitate. The service can also be purchased via an enterprise license agreement purchase order, or subscription purchasing program if States prefer to do so. As with vCloud Air Virtual Private Cloud On Demand, this offering includes access to the My VMware Account Management Console ("My VMware") and the VMware vCloud Air Console ("Console"). Both are described in detail above. VMware will also provide organization administrator access to the vCloud API.
VMware vCloud Air Networking	**Complies.** vCloud Air Networking services meet NIST on-demand self-service characteristics. vCloud Air consumers can unilaterally provision network resources with no human interaction. Customers can consume network resources by creating an account and building network workloads requiring no interaction with VMware to facilitate. Every vCloud Air service includes a connection to the Internet, one or more public IP addresses, and critical networking capabilities such as load balancing, a firewall, network address translation (NAT), and VPN connectivity via the Edge Gateway.
VMware vCloud Air Advanced Networking Services	**Complies.** vCloud Air Advanced Networking services meet NIST on-demand self-service characteristics. vCloud Air consumers can unilaterally provision advanced network resources with no human interaction. Customers can consume advanced network resources by creating an account and building advanced network workloads requiring no interaction with VMware to facilitate. As with vCloud Air Virtual Private Cloud On Demand, this offering includes access to the My VMware Account Management Console ("My VMware") and the VMware vCloud Air Console ("Console"). Both are described in detail above. VMware will also provide organization administrator access to the vCloud API.
VMware vCloud Air Direct Connect	**Not Applicable.** vCloud Air offers Direct Connect as an add-on service to the term-based core cloud subscription service. Available for OnDemand, Dedicated, Disaster Recovery, and Virtual Private Clouds, you can request Direct Connect ports through My VMware.
VMware vCloud Air Hybrid Cloud Manager	**Not Applicable.** vCloud Air Hybrid Cloud Manager is a tool that can be ordered as an add-on to manage cloud infrastructure. For Dedicated Clouds, it is offered through two subscription add-ons titled Hybrid Networking Standard and Hybrid Networking Premium. These options allow users to extend single or multiple vCenter connections to best meet their hybrid environment needs.
PC/Desktop "aaS": VMware Horizon Air Desktops and Apps	**Complies.** VMware Horizon Air Desktops and Apps service meets NIST on-demand self-service characteristics. VMware Horizon Air Desktops and Apps consumers must initially contact VMware to purchase a core desktop subscription service on a monthly or annual basis or prepaid for the life of the term.

Table 12. VMware On-Demand IaaS

6.1.2.1.b On-Demand Self Service Capabilities of VMware's Public SaaS Services

Table 13 provides proof that VMware's proposed Public SaaS services provide On-Demand Self-Service as defined by NIST. For details on each service discussed below, see VMware's proposed Public SaaS Catalog in section 6.1.3.b below.

VMware's Private, Hybrid and Community Cloud Offerings	Requirement
Software as a Service (SaaS)	**Service must meet the following NIST definition of On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
VMware AirWatch (All Products), VMware Workspace ONE, and VMware Identity Manager proposed below in section 6.1.3.b	**Complies.** All VMware SaaS products meet NIST on-demand self-service characteristics. Participating Entities can unilaterally provision VMware SaaS resources via an online portal with no human interaction. Customers can consume virtual desktop resources by creating an account and requesting virtual desktops paid via credit card requiring no interaction with VMware to facilitate. VMware Identity Manager Advanced Edition is available as part of AirWatch Blue and Yellow Management Suites and VMware Workspace ONE. VMware SaaS customers manage their device fleets through VMware consoles while VMware maintains the cloud environment, including computing resource allocation. We have dedicated personnel who monitor network and storage requirements to help ensure the availability of our SaaS offering. VMware establishes baselines as part of our formal Configuration Management and Change Management policies. AirWatch uses a combination of industry-recognized monitoring and alerting tools to secure the cloud environment.
SocialCast	**Complies.** VMware SocialCast meets NIST on-demand self-service characteristics. vCloud Air consumers can unilaterally provision SocialCast instances via an online portal with no human interaction. Customers can consume SocialCast resources by creating an account and requesting SocialCast paid via credit card requiring no interaction with VMware to facilitate
VMware vRealize Air Compliance	**Complies.** VMware vRealize Air Compliance meets NIST on-demand self-service characteristics. vCloud Air consumers can unilaterally provision vRealize Air Compliance instances via an online portal with no human interaction. Customers can consume vRealize Air Compliance resources by creating an account and requesting vRealize Air Compliance paid via credit card requiring no interaction with VMware to facilitate.

Table 13. VMware On-Demand SaaS

6.1.2.1.c On-Demand Self-Service Capabilities of VMware's Private, Hybrid, and Community IaaS Enablement Offerings

Table 14 provides proof that NIST's On-Demand Self-Service capabilities are not applicable to VMware's proposed Private, Hybrid, and Community IaaS Enablement Offerings. These tools will enable Participating Entities to establish their own On-Demand Self-Service capabilities within their own Private, Hybrid, and Community IaaS infrastructure. For details on each service discussed below see VMware's proposed Private, Hybrid, and Community IaaS Enablement Catalog in section 6.1.3.c below.

VMware's Private, Hybrid and Community Cloud Offerings	Requirement
Infrastructure as a Service (IaaS) Enablement	**Service must meet the following NIST definition of On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
All Products proposed in Section 6.1.3.c below	**Not Applicable.** These products are sold as downloadable software to the consumer. The consumer must then install and configure the software on their servers unless installation and configuration services are also purchased. These products enable to consumer to create an on premises private cloud which can then be connected to the public cloud or other private clouds to create a hybrid or community cloud. These products are necessary for the deployment of a private, hybrid, or community cloud as they enable the On Demand service and all other NIST key cloud criteria for the consumer. If desired, VMware professional services can be purchased to install and configure VMware vCloud Suite on behalf of the consumer.

Table 14. VMware On-Demand IaaS Enablement

6.1.2.2 NIST Characteristic - Broad Network Access: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how network access is provided. {8.1.2.2}

VMware Response:

The following tables explain how each service in the proposed catalog found below in sections 6.1.3.a - 6.1.3.c satisfies the NIST definition of Broad Network Access.

6.1.2.2.a Broad Network Access Capabilities of VMware's Public IaaS Services

Table 15 provides proof that VMware's proposed Public IaaS services provide Broad Network Access as defined by NIST. For details on each service discussed below, see VMware's proposed Public IaaS Catalog in section 6.1.3.a below.

VMware's Private, Hybrid and Community Cloud Offerings	Requirement
Infrastructure as a Service (IaaS)	**Service must meet the following NIST definition of Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
All IaaS products proposed in section 6.1.3.a (except vCloud Air Hybrid Manager, covered below)	**Complies.** All of these products meet NIST Broad Network Access characteristics. Their capabilities are available over the public internet and can be used by heterogeneous thin or thick client platforms. Consumers only need Internet access to access the IaaS products proposed in section 6.1.3.a (except vCloud Air Hybrid Manager, discussed below). Additional capabilities exist including the ability to secure communications over the public internet including IPSEC VPN, SSL Client VPN, and the ability to consume via private WAN connectivity. vCloud Air support ranges from the most basic, e.g., IPSEC VPN, to some of the most advanced capabilities related to broad network access, e.g., dynamic routing protocols including BGP and OSPF.
VMware vCloud Air Hybrid Cloud Manager	**Complies.** vCloud Air Hybrid Cloud Manager is designed to facilitate the management hybrid cloud which are by definition a public and private cloud connected by a network. vCloud Air Hybrid Cloud Manager is accessed through standard mechanisms via thin or think client platforms.

Table 15. VMware Broad Network Access IaaS

6.1.2.2.b Broad Network Access Capabilities of VMware's Public SaaS Services

Table 16 provides proof that VMware's proposed Public SaaS services provide or are not applicable to provide Broad Network Access as defined by NIST. For details on each service discussed below, see VMware's proposed Public SaaS Catalog in section 6.1.3.b below.

VMware's Private, Hybrid and Community Cloud Offerings	Requirement
Software as a Service (SaaS)	**Service must meet the following NIST definition of Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
All SaaS Products proposed in Section 6.1.3.b above	**Complies.** All of the listed products meet NIST broad Network Access characteristics. All of the proposed SaaS services are accessed over the Internet or private network through standard mechanisms via thin or think client platforms. Customers of these services need only a network connection and a modern web browser to access the AirWatch administrator console, SocialCast Portal, and vRealize Air. Our solution is network agnostic to provide a broad range of options for our customers. VMware provides redundant-configured, highly-available solutions to our SaaS customers to help ensure the confidentiality, integrity, availability, and broad network access of our hosted offering.

Table 16. VMware Broad Network Access SaaS

6.1.2.2.c Broad Network Access Capabilities of VMware's Private, Hybrid, and Community IaaS Enablement Offerings

Table 17 provides proof that NIST's Broad Network Access capabilities are not applicable to VMware's proposed Private, Hybrid, and Community IaaS Enablement offerings. These tools will enable Participating Entities to establish their own Broad Network Access capabilities within their own Private, Hybrid, and Community IaaS infrastructure. For details on each service discussed below, see VMware's proposed Private, Hybrid, and Community IaaS Enablement Catalog in section 6.1.3.c below.

VMware's Private, Hybrid and Community Cloud Offerings	Requirement
Infrastructure as a Service (IaaS) Enablement	**Service must meet the following NIST definition of Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
All Products proposed in Section 6.1.3.c above	**Not Applicable.** These products are sold as downloadable software to the consumer. The consumer must then install and configure the software on their servers unless installation and configuration services are also purchased. These products enable to consumer to create an on premises private cloud which can then be connected to the public cloud or other private clouds to create a hybrid or community cloud. These products are necessary for the deployment of a private, hybrid, or community cloud as they enable broad network access and all other NIST key cloud criteria for the consumer.

Table 17. VMware Broad Network Access IaaS Enablement

6.1.2.3 NIST Characteristic - Resource Pooling: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how resource pooling technical capability is met. {8.1.2.3}

VMware Response:

The following tables explain how each service in the proposed catalog found below in sections 6.1.3.a – 6.1.3.c satisfies the NIST definition of Resource Pooling.

6.1.2.3.a Resource Pooling Capabilities of VMware's Public IaaS Services

Table 18 provides proof that VMware's proposed Public IaaS services provide Resource Pooling as defined by NIST. For details on each service discussed below see VMware's proposed Public IaaS Catalog in section 6.1.3.a below.

VMware's Private, Hybrid and Community Cloud Offerings	Requirement
Infrastructure as a Service (IaaS)	**Service must meet the following NIST definition of Resource Pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, and network bandwidth.
All IaaS products proposed in section 6.1.3.a **(except vCloud Air Hybrid Manager, covered below)**	**Complies.** vCloud Air provides a pool of vCPU, vRAM, Network and Storage on the shared physical infrastructure. All multitenant vCloud Air offerings provide a logically isolated virtual data center ("VDC"). Based on vSphere resource isolation, physical resources are operating in a multitenant design, but tenants are given strict guarantees to their share of resources, and load is evenly balanced across the infrastructure, ensuring robust and scalable availability to everyone in the cloud. VMware vCloud Air Dedicated Cloud provides a dedicated single tenant environment that also meets this requirement in the following way: The vCloud Air Dedicated Cloud computing resources are pooled to serve multiple applications or organizations within a dedicated set of hardware. Although the resources are dedicated to a single organization (tenant), because multiple workloads, virtual machines, applications, business units, etc. share physical and virtual resources within the dedicated pool and they are dynamically assigned and reassigned according to consumer demand, it meets the spirit of this requirement. VMware vCloud Air provides the required location independence and requires that the customer directly specify location of the data center that will host their cloud at time of instantiation. This ensures that the customer's infrastructure and data remain in the geographic location or locations of their choice.
VMware vCloud Air Hybrid Cloud Manager	**Not Applicable**. vCloud Air Hybrid Cloud Manager is designed to facilitate the management of hybrid cloud. Resource pooling is not applicable to a tool such as VMware vCloud Air Hybrid Cloud Manager

Table 18. VMware Resource Pooling IaaS

6.1.2.3.b Resource Pooling Capabilities of VMware's Public SaaS Services

Table 19 provides proof that VMware's proposed Public SaaS services provide Resource Pooling as defined by NIST. For details on each service discussed below see VMware's proposed Public SaaS Catalog in section 6.1.3.b below.

VMware's Private, Hybrid and Community Cloud Offerings	Requirement
Software as a Service (SaaS)	**Service must meet the following NIST definition of Resource Pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
All SaaS Products proposed in above	**Not Applicable.** This NIST requirement is not relevant to SaaS offerings. As these are SaaS offerings, all infrastructure is abstracted from the user, thus resource pooling is not applicable to these products. In some cases, these SaaS products may share pools of infrastructure resource, in others, they may have dedicated resources. AirWatch manages computing resources to through defined policies and procedures to help ensure our 99.9% uptime SLA. We have personnel dedicated to establishing and monitoring storage, network, processing, etc. allocations. AirWatch leverages virtual technologies configured for high availability to support our Dedicated and Shared SaaS offerings. We can provide additional details regarding these technologies as conversations progress. Systems are configured and hardened according to industry best practices and vendor recommendations. Customers are isolated from each other in both Shared SaaS and Dedicated SaaS environments.

Table 19. VMware Resource Pooling SaaS

6.1.2.3.c Resource Pooling Capabilities of VMware's Private, Hybrid, and Community IaaS Enablement Offerings

Table 20 provides proof that NIST's Resource Pooling capabilities are not applicable to VMware's proposed Private, Hybrid, and Community IaaS Enablement offerings. These tools will enable Participating Entities to establish their own Resource Pooling capabilities within their own Private, Hybrid, and Community IaaS infrastructure. For details on each service discussed below see VMware's proposed Private, Hybrid, and Community IaaS Enablement Catalog in section 6.1.3.c below.

VMware's Private, Hybrid and Community Cloud Offerings	Requirement
Infrastructure as a Service (IaaS) Enablement	**Service must meet the following NIST definition of Resource Pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, and network bandwidth.
All Products proposed in section 6.1.3.c below	**Not Applicable.** These products are sold as downloadable software to the consumer. These products enable the consumer to create on premises private clouds. These products are necessary for the deployment of a private, hybrid, or community cloud as they enable resource pooling and all other NIST key cloud criteria for the consumer.

Table 20. VMware Resource Pooling IaaS Enablement

6.1.2.4 NIST Characteristic - Rapid Elasticity: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how rapid elasticity technical capability is met. {8.1.2.4}

VMware Response:

The following tables explain how each service in the proposed catalog found below in sections 6.1.3.a-6.1.3.c satisfies the NIST definition of Rapid Elasticity.

6.1.2.4.a Rapid Elasticity Capabilities of VMware's Public IaaS Services

Table 21 provides proof that VMware's proposed Public IaaS services provide Rapid Elasticity as defined by NIST. For details on each service discussed below see VMware's proposed public IaaS catalog in section 6.1.3.a below.

Public Cloud Offerings	Requirement
Infrastructure as a Service (IaaS)	**Service must meet the following NIST definition of Rapid Elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
All IaaS products proposed (except vCloud Air Hybrid Manager, covered below)	**Partially Complies.** All vCloud Air offerings provide a pool of vCPU, vRAM, Network and Storage on shared or dedicated physical infrastructure that can be elastically provisioned and released rapidly. However, the method of providing rapid elasticity varies among our proposed IaaS offerings. • **vCloud Air On Demand fully complies.** In the case of vCloud Air On Demand Cloud services, Capabilities can be elastically provisioned and released. It can be done automatically using tools such as vRealize Automation or similar products if the participating entity so desires. The capabilities of vCloud Air OnDemand appear to be unlimited from the end user's perspective. • **All other IaaS proposed in section 6.1.3.a partially complies**. Although these services must be purchased via a purchase order, subscription, or ELA, capacity can be increased and decommissioned at the request of the participating entity. The length of service will drive the time required to execute the scaling of each service.
VMware vCloud Air Hybrid Cloud Manager	**Not Applicable.** vCloud Air Hybrid Cloud Manager is designed to facilitate the management of hybrid cloud. Rapid Elasticity is not applicable to a tool such as VMware vCloud Air Hybrid Cloud Manager

Table 21. VMware Rapid Elasticity IaaS

6.1.2.4.b Rapid Elasticity Capabilities of VMware's Public SaaS Services

Table 22 provides proof that VMware's proposed Public SaaS services provide Rapid Elasticity as defined by NIST. For details on each service discussed below see VMware's proposed Public SaaS Catalog in section 6.1.3.b below.

Public Cloud Offerings	Requirement
Software as a Service (SaaS)	**Service must meet the following NIST definition of Rapid Elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
All SaaS Products	**Complies.** This NIST requirement is not relevant to SaaS offerings. SaaS infrastructure is abstracted from the user, thus rapid elasticity is not applicable to these products. However,

proposed in above	the participating entity is able to rapidly add users to the SaaS services to scale up in times of need. Similarly, user access rights can rapidly be removed as needed. The AirWatch solution was designed from day one with scalability in mind, and our flexible architecture allows us to grow with your business. The design of our technical architecture manifests itself best in large deployments, where greater granularity is required for effective management. With deployments and testing environments nearing 200,000+ simultaneous devices, our solution asserts itself over complex deployment needs through our single, web-based console. • Our configurable architecture is designed to easily support 25 to 100,000+ devices and any number of users. • We have numerous deployments of 20,000+ devices. • We have AirWatch Cloud environments supporting nearly 200,000 devices each.

Table 22. VMware Rapid Elasticity SaaS

6.1.2.4.c Rapid Elasticity Capabilities of VMware's Private, Hybrid, and Community IaaS Enablement Offerings

Table 23 provides proof that NIST's Rapid Elasticity capabilities are not applicable to VMware's proposed Private, Hybrid, and Community IaaS Enablement offerings. These tools will enable Participating Entities to establish their own Rapid Elasticity capabilities within their own Private, Hybrid, and Community IaaS infrastructure. For details on each service discussed below see VMware's proposed Private, Hybrid, and Community IaaS Enablement Catalog in section 6.1.3.c below.

VMware's Private, Hybrid and Community Cloud Offerings	Requirement
Infrastructure as a Service (IaaS) Enablement	**Service must meet the following NIST definition of Rapid Elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
All Products proposed in Section 6.1.3.c above	**Not Applicable.** The software products proposed in section 6.1.3.c above are sold as downloadable software to the consumer. These products enable the consumer to create on premises private clouds. These products are necessary for the deployment of a private, hybrid, or community cloud as they enable rapid elasticity and all other NIST key cloud criteria for the consumer.

Table 23. VMware Rapid Elasticity IaaS Enablement

6.1.2.5 NIST Characteristic - Measured Service: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how measured service technical capability is met. {8.1.2.5}

VMware Response:

The following tables explain how each service in the proposed catalog found below in sections 6.1.3.a – 6.1.3.c satisfies the NIST definition of Rapid Elasticity.

6.1.2.5.a Measured Service Capabilities of VMware's Public IaaS Services

Table 24 provides proof that VMware's proposed Public IaaS services provide or a not applicable to provide Measured Service as defined by NIST. For details on each service discussed below see VMware's proposed Public IaaS Catalog in section 6.1.3.a below.

Public Cloud Offerings	Requirement
Infrastructure as a Service (IaaS)	**Service must meet the following NIST definition of Measured Service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability[1] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. [1]Typically, this is done on a pay-per-use or pay-per-charge basis.
All IaaS products proposed in section 6.1.3.a (except vCloud Air Hybrid Manager, covered below)	**Complies.** VMware provides automatic monitoring and metering service to vCloud Air infrastructure, infrastructure networks, top-layer management and user-management interfaces, and computing, storage, and network hardware for availability, capacity, and performance. VMware also provides customers with a Virtual Data Center (VDC) and virtual machine (VM) level view of compute and storage resource utilization and availability. Resource usage can be monitored, controlled, and reported, providing transparency for both VMware and customers.
VMware vCloud Air Hybrid Cloud Manager	**Not Applicable**. vCloud Air Hybrid Cloud Manager is designed to facilitate the management of hybrid cloud. Metered Usage is not applicable to a tool such as VMware vCloud Air Hybrid Cloud Manager

Table 24. VMware Measured Service for IaaS

6.1.2.5.b Measured Service Capabilities of VMware's Public SaaS Services

Table 25 provides proof that VMware's proposed Public SaaS services provide Rapid Elasticity as defined by NIST. For details on each service discussed below see VMware's proposed Public SaaS Catalog in section 6.1.3.b below.

Public Cloud Offerings	Requirement
Software as a Service (SaaS)	**Service must meet the following NIST definition of Measured Service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability[1] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. [1]Typically, this is done on a pay-per-use or pay-per-charge basis.
All SaaS Products proposed in Section 6.1.3.b above	**Complies.** The SaaS products proposed provides metering of active devices or user accounts (depending on which licensing model the user chooses). These can be monitored, controlled, and reported providing transparency for both VMware and the participating entity (consumer of the utilized service.)

Table 25. VMware Measured Service for SaaS

6.1.2.5.c Measured Service Capabilities of VMware's Private, Hybrid, and Community IaaS Enablement Offerings

Table 26 provides proof that NIST's Measured Service capabilities are not applicable to VMware's proposed Private, Hybrid, and Community IaaS Enablement offerings. These tools will enable Participating Entities to establish their own Measured Service capabilities within their own Private, Hybrid, and Community IaaS infrastructure. For details on each service discussed below see VMware's proposed Private, Hybrid, and Community IaaS Enablement Catalog in section 6.1.3.c below.

Public Cloud Offerings	Requirement
Infrastructure as a Service (IaaS) Enablement	**Service must meet the following NIST definition of Measured Service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability[1] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. [1]Typically, this is done on a pay-per-use or pay-per-charge basis.
All Products proposed below in section 6.1.3.c	**Not Applicable.** These products are sold as downloadable software to the consumer. These products enable the consumer to create on premises private clouds. These products are necessary for the deployment of a private, hybrid, or community cloud as they enable measured Service and all other NIST key cloud criteria for the consumer. In particular, VMware vRealize Business Suite provides private clouds with measured service and the ability to establish pay-per-use, pay-per-charge business models.

Table 26. VMware Measured Service for IaaS Enablement

6.1.3 Offeror must identify for each Solution the subcategories that it offers for each service model. For example if an Offeror provides a SaaS offering then it should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc. {8.1.3}

VMware Response:

The following three sections (6.1.3.a - 6.1.3.c) identify each VMware service category. Service Categories are divided by offering type in accordance with **Attachment C**.

6.1.3.a VMware's Public Infrastructure as a Service (IaaS) Catalog

Table 27 lists the catalog for VMware's public cloud IaaS offerings. All services proposed in this section meet the NIST definitions of public cloud and of IaaS. In addition, some of these products can be used to enable hybrid clouds when coupled with VMware and other private cloud technologies.

Public Cloud Offerings
Infrastructure as a Service (IaaS)
On Demand Infrastructure as a Service
VMware vCloud Air Virtual Private Cloud OnDemand allows users to: • Purchase cloud infrastructure on demand • Scale up and down based on need or budget • Manage with the VMware tools they already own • Migrate workloads bi-directionally with zero application changes • Stand up new infrastructure in minutes • Benefit from no up-front resource size, capacity or cost commitments • Self-service provision resources • Scale via virtually unlimited resource pools • Create custom builds and live reallocations of any ratio of CPU, memory and storage • Take advantage of the flexibility of multiple virtual data centers • Turn static capital costs into variable operating, pay-as-you-go expenses • Leverage their existing VMware templates and processes • Run their applications onsite, offsite or in any combination with the ability to cancel at any time
Dedicated Infrastructure as a Service
VMware vCloud Air Dedicated Cloud: vCloud Air Dedicated Cloud is a single-tenant, physically isolated IaaS platform that is operated by VMware and compatible with your on premises vSphere environments for true Hybrid functionality. Dedicated Cloud is your own private cloud instance in the public cloud as it provides customers with

their own compute nodes for utmost security. This solution offers users the additional flexibility to assign resources to separate virtual data centers, each with individual user access controls. Dedicated Cloud includes compute resource reservation control—the entire compute and memory allocation is reserved and can be allocated or over-committed as you desire. Overcommit resources as you see fit, to best meet your performance needs.

Dedicated Cloud eases licensing, as many commercial software options are licensed per core. With Dedicated Cloud, you know the amount of cores and can accurately budget for licensing costs.

As with all services in the vCloud Air portfolio, Dedicated Cloud is an extension of your data center, allowing you to choose where your applications and workloads are hosted. Dedicated Cloud is configurable and can grow as your needs increase, including additional increments of compute, storage, bandwidth, data protection, and more. The Dedicated Cloud IaaS product is truly your own private cloud in the public cloud.

Virtual Private Infrastructure as a Service

VMware vCloud Air Virtual Private Cloud: VMware vCloud Air Virtual Private Cloud is a secure, vSphere compatible multi-tenant, Infrastructure as a service platform operated by VMware. Virtual Private Cloud is a high performance, highly available public cloud service that includes a pool of compute, storage and private networking resources. Virtual Private Cloud is compatible with other VMware based clouds, and offers seamless hybrid cloud capabilities including bi-directional workload portability, data center extension and hybrid networking.

Virtual Private Cloud is a cost-effective solution that is ideal for expanding your presence into the public cloud instead of expanding your onsite infrastructure. With its pool of highly available compute, storage, and networking resources, Virtual Private Cloud fits well in scenarios involving variable or bursting workloads and is optimal for test and development, or running production applications. The Virtual Private Cloud service can be expanded with various add-ons to enhance the solution to best fit your growing enterprise needs.

Government Infrastructure as a Service

VMware vCloud Government Service (vCGS) Dedicated Cloud: VMware vCloud Government Service provided by Carpathia, is an infrastructure-as-a-service hybrid cloud offer operating with a FedRAMP P-ATO issued by the Joint Authorization Board (JAB) giving you a common platform to extend your data center to the cloud. Carpathia is a trusted cloud operator and leading provider of hybrid cloud services and managed hosting, providing secure, reliable and compliant IT infrastructure and management for some of the world's most demanding enterprises and government agencies. Because vCloud Government Service is based on the same award-winning technology used by so many US government agencies today - vSphere - it gives you the flexibility to seamlessly run new and existing applications in the cloud, on premise, or both.

vCloud Government Service is an isolated community cloud designed to allow US government agencies and customers operating under a FedRAMP mandate to move sensitive workloads to the cloud while adhering to the compliance and regulatory requirements under which they operate.

vCloud Government Service dedicated cloud provides you with infrastructure that is physically isolated from all other vCloud Government Service tenants, giving you your own private cloud instance where cloud administrators can selectively extend self-service capabilities to internal teams for rapid provisioning of resources.

Government Virtual Private Infrastructure as a Service

VMware vCloud Government Service (vCGS) Virtual Private Cloud: VMware vCloud Government Service provided by Carpathia, is an infrastructure-as-a-service hybrid cloud offer operating with a FedRAMP P-ATO issued by the Joint Authorization Board (JAB) giving you a common platform to extend your data center to the cloud. Because vCloud Government Service is based on the same award-winning technology used by so many US federal agencies today - vSphere - it gives you the flexibility to seamlessly run new and existing applications in the cloud, on premise, or both.

vCloud Government Service is an isolated community cloud designed to allow US government agencies and customers operating under a FedRAMP mandate to move sensitive workloads to the cloud while adhering to the compliance and regulatory requirements under which they operate.

vCloud Government Service virtual private cloud provides you with logically isolated infrastructure, with fully private networking and resource pools and provides a lower initial capacity footprint.

Business Continuity/Disaster Recovery

VMware vCloud Air Disaster Recovery: Business continuity and disaster recovery are paramount for ensuring your business critical environment, data, and online presence are available with minimal downtime. The availability services offered on vCloud Air help ensure that your data is protected, recoverable, and accessible by you and your customers.

Customers know disaster recovery planning is an IT priority, but lack of proper planning, testing, and resources puts you at risk of losing crucial operational information and incurring revenue loss. If you are looking for a cost-

efficient and agile solution to implement or to replace dated, complex, and/or costly plans, VMware vCloud Air Disaster Recovery, built on VMware vSphere Replication, provides a cloud-based failover environment for dependable recovery when faced with an operational disruption. Asynchronous replication at the hypervisor layer allows for virtual machines (VMs) in VMware vSphere to be easily configured for disaster recovery.

Data Protection

VMware vCloud Air Data Protection: The need to protect workloads is the same whether it's onsite or in the cloud. You can ensure business continuity in your vCloud Air environment with vCloud Air Data Protection, an optional backup and recovery feature for Dedicated Cloud or Virtual Private Cloud instances.

Data Protection is an agent-less, self-service, policy-driven backup and recovery service with image-level backups to ensure all operating system, file system and application data residing within a virtual machine are captured as a snapshot image before committed to backup media. With this self-service backup feature, you can fully embrace the public cloud and deploy critical applications without worrying about data loss.

Data Replication

VMware Continuent: VMware Continuent provides data replication between relational databases and to data warehouses and analytics engines, enabling users to derive insight from big data to make better business decisions. In addition, VMware Continuent allows enterprises running business-critical database applications to affordably achieve globally redundant disaster recovery (DR), commercial-grade high availability (HA), and performance scaling. VMware Continuent makes it simple to create database clusters in the cloud or in your private data center and between these locations, to keep the data available even when systems fail.

Benefits provided by Continuent are:

- Flexible, High-Performance Replication for Oracle and MySQL Databases: Replicate data from Oracle to Oracle, Oracle to MySQL, MySQL to Oracle, and from MySQL to MySQL.
- Disaster Recovery: Recover quickly and automatically from DBMS and host failures.
- Replication between RDBMs and to Analytics and Big Data: Replicate quickly and efficiently between relational databases and to data warehouses and analytics engines to derive insight from big data for better business decisions.
- High Availability: Replace a failed primary DBMS server within seconds while maintaining continuous availability without losing transactions.

Storage: Block Storage

VMware vCloud Air Block Storage: vCloud Air is a dynamic public cloud platform that offers high performance, reliable storage options to fit varying workload needs. With the purchase of any of our core compute services, you can choose from two different persistent block storage types for vCloud Air.

SSD-Accelerated Storage: SSD-Accelerated storage is our highest performing SSD cached storage option.

- Recommended for workloads that require the highest IOPS performance
- SSD-Accelerated storage is highly recommended for tier one, two, and three workloads, including high-performance database applications where fast update times are critical

Standard Storage: Standard Storage is ideal for virtual machines that do not require the highest performance.

- Persistent block storage solution that is tailored to be cost-effective, yet high-performing, meeting the needs of all but the highest IOPs requirements
- Ideal for tier two and three workloads, like test and development, disaster recovery and web servers. It is also recommended for larger, static data sets

Whether you choose Virtual Private Cloud, Dedicated Cloud or OnDemand as your compute solution, you have access to the same storage volumes and you can choose whether you want the highest performance SSD-Accelerated Storage or the more cost-conscious Standard Storage. Both options allow for effortless growth of virtual machine disks without downtime and the flexibility to migrate easily from one option to the other as needed. By using a tiered storage approach with your vCloud Air instance, you have the ability to divide workloads in your environment based on your performance requirements and you can dynamically blend storage types to best fit workload requirements.

The Dedicated Cloud core subscription includes 6TB of storage and the Virtual Private Cloud core subscription includes 2TB of storage. At the time of purchase, you can specify which type of storage you would like for your compute solution. As your environment grows or requirements shift, you can simply add more storage and select your storage tier as needed.

Storage: Object Storage
VMware vCloud Air Object Storage: VMware vCloud Air Object Storage offers an extremely scalable, cost - effective, and dependable cloud - based storage solution for unstructured data. The service is simple to use, easy to setup, provides global scale and has built - in resiliency. Easily scale up to petabytes and generate real - time intelligence from custom meta - data with vCloud Air Object Storage. VMware offers VMware vCloud Air Object Storage powered by Google Cloud Platform which provides three storage options: • Standard Storage • Durable Reduced Availability (DRA) Storage • Nearline Storage
Networking
VMware vCloud Air Networking: Cloud networking is an essential component of cloud computing and forms the foundation for the hybrid cloud. Unlike offerings from other leading cloud providers, VMware vCloud Air provides essential networking infrastructure at no additional cost. Every vCloud Air service includes a connection to the Internet, one or more public IP addresses, and critical networking capabilities such as load balancing, a firewall, network address translation (NAT), and VPN connectivity via the Edge Gateway. Additionally, Advanced and Hybrid Networking Services are available to enhance the standard included networking capabilities. Direct Connect is also available if you are looking for higher speed, secure private line connectivity or if you are cross-connecting to co-located infrastructure.
Advanced Networking Services
VMware vCloud Air Advanced Networking Services: Advanced Networking Services deliver enterprise-grade networking and security capabilities powered by VMware NSX technology, providing zero trust security in the cloud. Re-invent security in the public cloud and improve network manageability, while providing a path to true hybrid networking across your onsite vSphere data center to the cloud. The following features are available via VMware vCloud Air Advanced Networking Services: **Granular Network Security:** Enables Trust Groups powered by distributed firewalls to be deployed and attached to applications, following the application anywhere it goes in the cloud. **Network Scalability:** Supports up to 200 routed network segments in a single virtual data center, enabling replication of complex on-premises network topologies in the cloud. **Dynamic Routing:** Support for Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) routing for continuity in cloud-hosted applications. **High Capacity Connectivity:** High capacity point-to-site SSL and site-to-site IPsec VPN options enable dozens of mobile devices and on-premises locations to securely connect into a single virtual data center. Enhanced Load Balancing: HTTPS and SSL termination support enterprise production workloads in the cloud.
Networking: Direct Link
VMware vCloud Air Direct Connect: Direct Connect is an additional method of connecting into a vCloud Air instance beyond standard Internet-based traffic and IPsec VPN tunnels. It provides the ability to create a high-throughput, dedicated link from your data center – either located remotely or within the same colocation facility – into your instance of vCloud Air. Direct Connect is jointly delivered by VMware and your Network Service Provider (NSP). VMware provides a 1 or 10 Gbps port connection and cross connect from the vCloud Air instance to the NSP's network termination point in a vCloud Air location; the NSP provides the dedicated network link from the termination point back to your data center. Direct Connect Enables: • High-Throughput Connection for Distributed Hybrid Applications • Direct Path for Performance-Sensitive Workloads • Secure Multi-Point Connections • Service Flexibility VMware offers two types of Direct Connect services: **VMware vCloud Air Direct Connect with Cross Connect:** Direct Connect with Cross Connect supports both site-to-site private line connectivity as well as cross-connections from co-located infrastructure. Benefits:

• Fast, dedicated connectivity: 1 or 10 Gbps options • Streamlined provisioning and billing: We provide the port and cross connect to simplify your billing relationships • Supports advanced and hybrid networking **VMware vCloud Air Direct Connect for Network Exchange:** Direct Connect for Network Exchange supports network exchange-based connections from on-premises data centers into vCloud Air. Benefits: • Dedicated connectivity: 1 or 10 Gbps options • Fastest time-to-value • Access advanced and hybrid networking • Supports additional value-added services from NSPs (varies by NSP)
Networking: Hybrid Networking
VMware vCloud Air Hybrid Cloud Manager: Seamlessly extend your on-premises vSphere powered data center into vCloud Air with vCloud Air Hybrid Cloud Manager. The Hybrid Cloud Manager offers hybrid networking and bi-directional workload migration capabilities, simplifying on and off-premises resource integration and management of workloads. • **Bi-Directional Workload Portability:** Seamless move workloads to and from vCloud Air using vSphere web client. • **Network Extension:** Data Center Extension through Layer 2 VPN. The Hybrid Cloud Manager feature is available for use with vCloud Air Dedicated Cloud.
PC/Desktop "aaS"
VMware Horizon Air Desktops and Apps: VMware Horizon Air Desktops and VMware Horizon Air Apps simplify the delivery of Windows desktops and applications as a cloud service. With VMware Horizon Air Desktops and Horizon Air Apps, the service provides: • Unified desktop and application access from the cloud on any device, including tablets, smartphones, laptops, PCs, thin clients, and zero clients. • Fully managed enterprise service. VMware manages the operations of the underlying infrastructure, while providing best-in-class service, support, and SLAs. • Built-in security capabilities such as secure point-to-point network connectivity, dedicated compute, and network isolation. Benefits of VMware Horizon Air Desktops and Apps are: • Support End Users with a Premium Experience: End users can access their virtual desktops and hosted apps from any device, anywhere, with the Horizon Client or through the web. • Reduce Costs: Reduce your upfront costs and lower your desktop total cost of ownership with predictable cloud economics that enable you to move from CapEx to OpEx. • Take Advantage of Built-In Security and Control: Deploy and manage cloud-hosted desktops and apps from a single console with built-in security options. • Leverage Your Existing Infrastructure Investment: Seamlessly extend your corporate datacenter to your cloud-hosted desktops and apps, while leveraging your corporate infrastructure resources.

Table 27. VMware IaaS Catalog

6.1.3.b VMware's Public SaaS Services Catalog

Table 28 lists the catalog for VMware's Public Cloud SaaS offerings. All services proposed in this section meet the NIST definitions of Public Cloud and Software as a Service.

Public Cloud Offerings
Software as a Service (SaaS)
Mobile Device Management
VMware AirWatch Mobile Device Management: AirWatch Mobile Device Management enables businesses to address challenges associated with mobility by providing a simplified, efficient way to view and manage all devices from the central admin console. Our solution enables you to enroll devices in your enterprise environment quickly, configure and update device settings over-the-air, and secure mobile devices.
Container Management

VMware AirWatch Container Management: AirWatch Container Management provides complete separation of corporate and personal data on devices, securing corporate resources and maintaining employee privacy. AirWatch enables organizations to standardize enterprise security and data loss prevention strategies across mobile devices through our flexible approach to containerization.
Mobile Application Management
VMware AirWatch Application Management: VMware AirWatch Mobile Application Management addresses the challenge of acquiring, distributing, securing and tracking mobile applications. Easily manage internal, public and purchased apps across employee-owned, corporate-owned and shared devices from one central console.
Mobile Content Management
VMware AirWatch Content Management: AirWatch Mobile Content Management enables secure mobile access to content anytime, anywhere. AirWatch Content Locker protects your sensitive content in a corporate container and provides users with a central application to securely access the latest sales materials, board books or financial reports from their mobile devices.
Mobile Email Management
VMware AirWatch Content Management: VMware AirWatch Mobile Email Management delivers comprehensive security for your corporate email infrastructure. With AirWatch, you can control which mobile devices access email, prevent data loss, encrypt sensitive data, enforce advanced compliance policies and allow users to easily sync email through the self-service portal. AirWatch supports native email clients, enterprise services, cloud-based clients, as well as our own client.
Mobile Browsing Management
VMware AirWatch Browsing Management: AirWatch Mobile Browsing Management enables secure browsing and provides organizations with the ability to configure customized settings to meet their unique business and end-user needs. AirWatch Browser allows administrators to define and enforce secure browsing policies from the admin console.
Telecom Management
VMware AirWatch Telecom Management: With the exponential growth of mobile devices, organizations need an effective way to track and monitor voice, SMS and data usage. Excessive usage can be a huge cost to organizations, and paying for an under-utilized service plan is wasteful. Monitoring telecom usage as well as compliance with service plan limits is required, and IT must also consider employee privacy when implementing a solution. VMware AirWatch Telecom Management enables IT to easily monitor data, voice and roaming usage alongside devices from the admin console. With AirWatch, IT has insight into telecom usage to help save time, money and resources. Roaming restrictions, automated compliance enforcement and self-service options for end users simplify telecom management for IT.
Laptop Management
VMware AirWatch Laptop Management: Access to mobile email is essential for employees who need to work on the go, however corporate email often contains sensitive data and documents. Companies need to ensure their mobile email strategy keeps data secure while providing an intuitive experience for end users. VMware AirWatch Mobile Email Management delivers comprehensive security for corporate email infrastructures. Email security requirements vary for organizations, depending on supported device ownership models and industry regulations. AirWatch offers flexible options for your email management strategy, giving you choice over the deployment strategy that best fits your business and security requirements. Integration with existing email infrastructures ensures you are maximizing your technology investments. Access to corporate email can be configured through the native device client or VMware AirWatch Inbox, a secure email container.
Rugged Device Management
VMware AirWatch Rugged Device Management: From warehouse operations to inventory tracking, logistics to field employees, rugged devices are an essential part of doing business. Today, IT must manage multiple rugged operating systems and device types, along with smartphones, tablets and laptops in the enterprise. VMware AirWatch Rugged Device Management enables you to manage rugged devices alongside your smartphones, tablets and laptops in a single console. AirWatch provides complete mobility management solutions for ruggedized devices. AirWatch supports native and OEM-specific Android operating systems, including versions 2.3+ and Windows Mobile 5, 6 and 7. AirWatch supports all major OEMs, including Datalogic, Honeywell, Pidion, Samsung and Zebra Technologies.

Multiuser Management
VMware AirWatch Multiuser Management: Mobile devices are revolutionizing the way that businesses operate, how students learn and the methods doctors employ to treat patients. Since deploying a device to each user can be cost-prohibitive, many organizations deploy devices to be shared by multiple users. Shared devices present increased security and device management challenges, and IT administrators must ensure that devices are secure and each user receives the restrictions, apps and content they need. VMware AirWatch Multiuser Management helps organizations across all industries address the challenges of shared devices. AirWatch helps meet enterprise security and management requirements for shared devices while providing the personalized experiences that users demand.
Collaboration
AirWatch Content Locker: Employees need anytime, anywhere access to corporate content to stay productive. Many employees are taking advantage of free file sharing services to access sensitive documents, putting your organization's corporate data at risk. The proliferation of consumer mobility is driving the need for a simple and ubiquitous content collaboration solution. AirWatch by VMware enables secure mobile access to content anytime, anywhere. AirWatch Content Locker protects your sensitive content in a corporate container and provides users with a central application to securely access, distribute and collaborate on the latest documents from their mobile devices.
Video Management
AirWatch Video: Video is playing an increasingly important role in the way people share information. Videos are easy to make and simple to consume. As enterprises video for company initiatives including employee communications, training and sales instruction, IT must support and secure global video distribution across multiple device platforms. AirWatch Video simplifies video distribution, user engagement, and security and management for the enterprise. Integration with content delivery network providers enables organizations to scale company-wide video initiatives. The intuitive presentation-ready interface makes it easy for end users to browse available videos and consume video content from their mobile devices. Easy management simplifies content assignment, analytics and security for IT.
Secure Enterprise Social Networking
Socialcast: Socialcast by VMware is the secure enterprise social networking platform that brings people, conversations, and projects together in a single place so employees can work better, find information faster, and get more done. Thousands of companies around the world use Socialcast as a modern way to connect and communicate. By organizing the day-to-day flow of work into a single location, accessible from anywhere, on any device, SocialCast allows employees to discover new people and ideas, work smarter, and focus on what is most important.
Identity Management
VMware Identity Manager: In today's world, applications and information are everywhere, both inside and outside the walls of your datacenter. IT departments are under more pressure than ever to secure and manage this new, changing landscape. Old methods of deploying applications are complex and often ineffective, relying heavily on domain-joined desktops and general-purpose VPN access. VMware Identity Manager administers the complete user lifecycle across the hybrid cloud complete with a custom app store, user provisioning, and application usage analytics to monitor and manage resources. In the mobile cloud era, VMware Identity Manager is the ideal solution, delivering the first mobile cloud identity management platform that federates user accounts for SaaS, web, and native mobile applications requiring no change to the application and solving a major roadblock to mobile application adoption in the enterprise.
Enterprise Mobility Management, Virtual Apps and Desktops, and Identity Management Suite
VMware Workspace ONE: VMware Workspace ONE is the result of innovative integrations of VMware Identity Manager, AirWatch Enterprise Mobility Management Suite, and Horizon Air now delivered through the Workspace ONE app to employees. While the standalone products remain available, many features are unique to the new Workspace ONE product line. The following are example use cases for adopting Workspace ONE: • A true BYO-anything (Bring-Your-Own-Anything) solution that gives employees flexibility and device choice while securing corporate data • A unified enterprise app store with seamless single sign-on across Windows apps, SaaS/Web apps, and native mobile apps

• Comprehensive Windows 10 management and deployment in the enterprise including real time Windows apps delivery • Accelerate Office 365 deployments by federating between existing on-premises Active Directory and Microsoft Azure Active Directory For Additional details on the products that comprise the VMware Workspace ONE, see the AirWatch, VMware Horizon, and VMware Identity Manager catalog items above.
Compliance
VMware vRealize Air Compliance: vRealize Air Compliance allows you to gain real-time visibility into security and compliance of your vSphere virtual infrastructure against the vSphere Hardening Guide as well as regulatory standards such as HIPAA and PCI. vRealize Air Compliance SaaS solution continuously monitors the configuration of your vSphere virtual infrastructure and alerts on changes, in real-time, that are non-compliant. The service delivers the visibility and actionable information you need, including who made the change and when, to immediately resolve any issues to maintain continuous compliance and improve security. Capabilities of vRealize Air Compliance include: **Configuration Compliance Management:** Enable continuous compliance - discover, measure, remediate and manage the compliance of your infrastructure in real-time, not monthly or quarterly. • Automatically discover and pinpoint vulnerabilities within the configuration of your virtual infrastructure • Assess infrastructure against a variety of out of the box security and regulatory policies (vSphere Hardening Guidelines, PCI, HIPAA and more) • Centralized, real-time insight into your state of compliance • Clearly understand the severity and risks of your infrastructure configuration **Compliance Monitoring:** Address risks before they are a problem through continuous compliance scan across your entire virtual infrastructure to ensure maximum compliance. • Event-driven configuration change detection • Real-time notifications of non-compliant changes • Capture important change information including time and person responsible • Create and manage policy exceptions on the fly **Audit and Report on Compliance:** Prove that IT is in control by ensuring up-to-date and accurate measurement of the virtual infrastructure against security and regulatory policies. • Real-time compliance dashboards with drill-down • Compliance scorecards to measure your state of compliance • Track compliance over time, measure improvement • Run reports on-demand for Auditors

Table 28. VMware SaaS Catalog

6.1.3.c VMware's Private, Hybrid and Community Cloud Catalog

Table 29 lists the catalog for VMware's private, hybrid, and community cloud enablement offerings. All products proposed in this section can be leveraged to build a private or community Infrastructure as a Service offerings as defined by NIST. In addition, they can be coupled with VMware and other public cloud services to meet the NIST definition of hybrid cloud.

VMware's Private, Hybrid and Community Cloud Offerings
Infrastructure as a Service (IaaS)
IaaS Suite
VMware vCloud Suite: VMware vCloud Suite enables IT to build and manage a vSphere–based private cloud resulting in strategic IT outcomes. It does this by assembling an integrated set of products, engineered to work better together, which provide: (1) infrastructure virtualization, (2) disaster recovery and testing automation, and (3) cloud management for on-premises vSphere environments. VMware vCloud Suite contains these integrated products: **Infrastructure Platform** • VMware vSphere: Industry leading server virtualization platform.

- Disaster Recovery Automation with VMware vCenter Site Recovery Manager: Policy-based disaster recovery and testing for all virtualized applications.

Cloud Management Platform

- VMware vRealize Operations: Intelligent performance, capacity, and configuration management for vSphere environments.
- VMware vRealize Automation: Self-service and policy-based infrastructure and application provisioning for vSphere environments.
- VMware vRealize Business: Automated costing, usage metering, and service pricing of virtualized infrastructure for vSphere environments.

See below for details on the component products that comprise the vCloud Suite.

Cloud Management Platform

VMware vRealize Suite: VMware vRealize Suite is a cloud management platform purpose-built for the hybrid cloud, delivering and managing infrastructure and applications quickly while maintaining IT control.

It provides a comprehensive management stack for IT services on VMware vSphere and other hypervisors, physical infrastructure, OpenStack and external clouds such as VMware vCloud Air and Amazon Web Services, all with a unified management experience.

Key Benefits:

- Automation: Automate the delivery and lifecycle management of infrastructure and application services while maintaining policy-based control
- Intelligent operations: Proactively manage performance, capacity, compliance, and logs across applications and infrastructure
- Business insight: Align IT spending with business priorities by getting full transparency of infrastructure and application service cost and quality.
- Unified management: Provision and manage IT services across private and public clouds with a consistent management experience
- Open platform: Extend management to third-party systems and leverage existing investments with open APIs, management packs, orchestration tools, and software development kits

VMware vRealize Suite is available in two editions:

VMware vRealize Suite Advanced

Comprehensive management solution for provisioning and ongoing management of infrastructure services:

- Rapid, self-service infrastructure provisioning
- Infrastructure health, performance, and capacity monitoring across physical, virtual, and hybrid cloud deployments
- Rapid creation of rate cards and automatic pricing of service catalog blueprints for use in a self-service portal
- Out-of-the-box benchmarks, usage metering, and public cloud comparison
- Plan, control, and recover costs expended in providing full IT Services stack, implementing cost transparency, cost optimization, and demand management
- Visibility into application dependencies and hypervisor change and configuration management

VMware vRealize Suite Enterprise

Complete management solution for deployment, ongoing management, and compliance for infrastructure and applications, with the following additional benefits:

- Rapid, self-service infrastructure and application provisioning
- Automated configuration and deployment of multitier cloud applications
- Visibility into application performance
- Regulatory compliance, OS-level change, and configuration management
- IT service level management
- Transparency into IT performance and value measures for all services and vendors, enabling IT to govern contractual commitments

VMware vRealize Suite consists of the following products:

- VMware vRealize Automation Advanced or Enterprise
- VMware vRealize Operations Advanced or Enterprise
- VMware vRealize Log Insight
- VMware vRealize Business Standard
- VMware vRealize Business Advanced or Enterprise

Cloud Automation

VMware vRealize Automation: VMware vRealize Automation empowers IT to accelerate the delivery and ongoing management of personalized, business-relevant infrastructure, application and custom services while improving overall IT efficiency. Policy-based governance and logical application modeling assures that multi-vendor, multi-cloud services are delivered at the right size and service level for the task and that needs to be performed. Full lifecycle management assures resources are maintained a peak operating efficiency.

Key features of vRealize Automation are:

Deliver a Personalized Self-service Experience

- Unified IT service catalog – deliver infrastructure, application and custom services
- Personalized, policy-based governance ensures the right
- service level to meet specific business needs
- Automation accelerates IT service delivery

Deploy Across Multi-Vendor, Hybrid Cloud Infrastructure

- Provide investment protection for current and future technology choices
- Deliver governance and control to enable hybrid cloud deployments
- Flexibility to choose the right cloud platform and location that meets the business needs

Unified Blueprint Model and Design Canvas

- Streamline the design process by assembling applications from pre-built components using a visual canvas with a drag and drop interface
- Blueprints as Code - Export, import and edit automation blueprints as text
- Leverage library of VMware and partner-provided blueprints

Simplify Application Release Automation with vRealize Code Stream

- Pipeline Automation – Model any release process for any kind of software
- Artifact Management – Assure the right artifact versions for each release
- Release Dashboard – Get full visibility into your release process
- Extensibility Framework – Leverage existing tools and processes

Achieve the Quickest Time to Value via an Extensible Automation Platform

- Comprehensive purpose-built functionality and broad multi-vendor, multi-cloud support built-in.
- Adapt and extend vRealize Automation comprehensive, purpose-built functionality
- Automate the delivery of any IT services
- Leverage VMware and partner-provided solutions in VMware Cloud Management Marketplace

Cloud Operations Management

VMware vRealize Operations: VMware vRealize Operations delivers intelligent operations management across physical, virtual, and cloud infrastructure—from VMware vSphere and Hyper-V to Amazon Web Services. It correlates data from applications to storage in a unified, easy-to-use management tool that provides control over performance, capacity, and configuration, with predictive analytics driving proactive action, and policy-based automation.

Traditional operations management systems do not meet the requirements of today's virtual and cloud infrastructure. They make IT too reactive because they lack the intelligence to aggregate, correlate, and analyze metrics across applications and infrastructure stacks.

vRealize Operations is built on a scale-out, resilient platform designed to deliver intelligent operational insights to simplify and automate management of applications and infrastructure across virtual, physical and cloud environments—from vSphere to Hyper-V, Amazon Web Services (AWS), and more.

vRealize Operations delivers:

- Intelligent operations – Self-learning tools, predictive analytics, intelligent workload management, and Smart Alerts about application and infrastructure health enable proactive identification and remediation of emerging performance, capacity, and configuration issues.
- Policy-based automation – Out-of-the-box and customizable policies for critical IT operations are associated with Smart Alerts, guided remediation, and compliance standards to deliver recommendations, or trigger actions, that optimize performance and capacity and enforce configuration standards.
- Unified management – An open and extensible platform, supported by third-party management packs for Microsoft, SAP, and others, provides complete visibility in a single console across applications, storage, and network devices.

Cloud Log Management
VMware vRealize Log Insight: VMware vRealize Log Insight delivers real-time log management for VMware environments, with machine learning-based Intelligent Grouping, high- performance search, and better troubleshooting at scale across physical, virtual, and cloud environments. With an integrated cloud operations management approach, it provides the operational intelligence and enterprise-wide visibility needed to proactively enable service levels and operational efficiency in dynamic hybrid cloud environments. Log Insight includes the following key capabilities: • Collects and analyzes all types of machine-generated log data, e.g., application logs, network traces, configuration files, messages, performance data, system state dumps, and more. • Enables administrators to connect to everything in their environment, e.g., OS, apps, storage, network devices, providing a single location to collect, store, and analyze logs at scale. • Features an intuitive interface that makes it easy to run interactive searches as well as deep analytical queries for quick, actionable insights. • Includes cluster technology to support log analytics at scale. • Automatically chooses the best visualization for your data, saving you time. • Adds structure to unstructured log data, enabling administrators to troubleshoot quickly, without needing to know the data beforehand. • Delivers real-time monitoring, search, and log analytics, coupled with a dashboard for stored queries, reports, and alerts, enabling correlation of events across the IT environment. • Helps users find virtual infrastructure problems with the addition of Intelligent Grouping, a machine-learning technology that can group related data together to aid in detecting problems rapidly. • Built-in knowledge of vSphere and other VMware products, like VMware Horizon with View, vRealize Operations and vRealize Automation. • VMware and third-party extensions available on VMware Solution Exchange. • Integrates with VMware vRealize Operations to bring unstructured and structured data together, for significantly enhanced end-to-end operations management. Business Benefits: • IT organizations using vRealize Log Insight can benefit from • Faster time-to-value, enabled by a powerful, intuitive, easy-to use interface. • Lower operating expenses and higher operational efficiency, from significant reduction in troubleshooting times, improved mean-time-to-resolution, and reduced manual e ort. • Predictable pricing model that includes unlimited amount of data and does not require buying licenses based on peak-usage and worst-case scenarios. • ROI and value maximization, by using Log Insight with vRealize Operations, bringing together best-of-breed tools for comprehensive operations management.
Cloud Business Management
VMware vRealize Business: VMware vRealize Business provides transparency and control over the cost and quality of IT services. By providing a business context to the services IT offers, vRealize Business helps IT organizations shift from a technology orientation to a service broker orientation, delivering a portfolio of IT services that align with the needs of line-of-business (LOB) stakeholders. vRealize Business provides the business management capabilities necessary to manage the business aspects of today's emerging hybrid cloud environments, helping to facilitate IT transformation, enabling customers to reduce capital and operating expenses and improve service delivery performance. Key Capabilities of vRealize Business include: • Data Integration: The foundation for vRealize Business is a robust enterprise platform providing broad functionality in a secure and scalable way. Data collected from private/hybrid cloud or from a vast array of third-party offerings is cleansed and validated before being added. In addition, vRealize Business includes an observation engine that monitors costs and quality to highlight changes that might require special attention. Furthermore, integration with the VMware portfolio of products enables direct metering and costing of cloud usage and calculation of overall public, private and hybrid costs. • Service Costing: vRealize Business provides powerful cost modeling capabilities allowing you to allocate or translate IT costs to each IT and Business Service. Supporting simple allocations to usage-based and complex activity-based costing. This approach provides superior control, agility and transparency compared to inference approaches whose algorithms offer you little control. • Planning and Budgeting: vRealize Business automates the manual processes of planning and budgeting. By consolidating and centralizing budgets, IT finance saves time and can appropriately rationalize budgets and allocations, provide transparency into planned versus actual spending and

variances, and track accumulated savings.
- Scenario Planning and Forecasting: What-if scenarios are used to evaluate, compare, plan and optimize spending decisions, enabling fact-based decision making. vRealize Business can show how overall costs, service costs and specific business unit costs would be affected by changing the environment, for example, from private to public cloud.

Software Defined Networking

VMware NSX: VMware NSX is the leading network virtualization platform that delivers the operational model of a virtual machine for the network. Similar to virtual machines for compute, virtual networks are programmatically provisioned and managed independent of underlying hardware. NSX reproduces the entire network model in software, enabling any network topology—from simple to complex multi-tier networks—to be created and provisioned in seconds. It enables a library of logical networking elements and services, such as logical switches, routers, firewalls, load balancers, VPN, and workload security. Users can create isolated virtual networks through custom combinations of these capabilities.

NSX exposes a RESTful API, allowing cloud management platforms to automate the delivery of network services. Network provisioning, which used to take days or weeks, now takes seconds. Because network services are now delivered to applications by the virtual network, no manual reconfiguration of physical network devices is necessary.

NSX Service Composer offers a way to automate the consumption of services and their mapping to virtual machines using logical policy. Customers can assign policies to groups of virtual machines and as more virtual machines are added to the group, the policy is automatically applied to the virtual machine. Customers can build advanced work flows automating security, compliance and network provisioning including load balancing and firewall rules.

NSX offers a platform to insert other vendor services. Integrated software and hardware partner products can range from network gateway services, application delivery services, and network security platforms to security services.

Key Features of NSX:

- Logical Switching – Reproduce the complete L2 and L3 switching functionality in a virtual environment, decoupled from underlying hardware
- NSX Gateway – L2 gateway for seamless connection to physical workloads and legacy VLANs
- Logical Routing – Routing between logical switches, providing dynamic routing within different virtual networks.
- Logical Firewall – Distributed firewall, kernel enabled line rate performance, virtualization and identity aware, with activity monitoring
- Logical Load Balancer – Full featured load balancer with SSL termination.
- Logical VPN – Site-to-Site & Remote Access VPN in software
- NSX API – RESTful API for integration into any cloud management platform

NSX Use Cases

NSX is the ideal solution for data centers with more than 500 virtual machines. NSX delivers immediate benefits for innovative multi-tenant cloud service providers, large enterprise private and R&D clouds and multi-hypervisor cloud environments. Typical use cases:

- Data Center Automation
- Speed up network provisioning
- Simplify service insertion – virtual and physical
- Streamline DMZ changes
- Self-Service Enterprise IT
- Rapid application deployment with automated network and service provisioning for private clouds & test/dev environments
- Isolated Dev, test and production environments on the same physical infrastructure
- Multi-tenant clouds
- Automate network provisioning for tenants with customization and complete isolation
- Maximize hardware sharing across tenants

Software Defined Storage

VMware Virtual SAN: VMware Virtual SAN is VMware's software- defined storage solution for Hyper-Converged Infrastructure (HCI). Seamlessly embedded in the hypervisor, Virtual SAN delivers enterprise-ready, high-performance shared storage for VMware vSphere Virtual Machines. It leverages commodity x86 components that easily scale to drastically lower TCO by up to 50%. Seamless integration with vSphere and the entire VMware

stack makes it the simplest storage platform for virtual machines—whether running business-critical applications, virtual desktops or remote server room apps.

Hybrid Cloud Management Enablement

vRealize Operations and Automation Public Cloud Extensions (available as add-ons to vCloud Suite): This add-on to VMware vCloud Suite extends vRealize Operations and Automation capabilities of vCloud Suite from private vSphere infrastructure to vCloud Air, Amazon Web Services or Microsoft Azure. For additional details see descriptions of vRealize Operations and vRealize Automation above.

Virtualization Infrastructure

VMware vSphere: VMware vSphere, the industry-leading virtualization platform, empowers users to virtualize any application with confidence, redefines availability and simplifies the virtual data center. The result is a highly available, resilient, on-demand infrastructure that is the ideal foundation of any cloud environment. This can drive down data center cost, increase system and application uptime, and drastically simplify the way IT runs the data center. vSphere is purpose-built for the next generation of applications and serves as the core foundational building block for the Software-Defined Data Center.

vSphere accelerates the shift to cloud computing for existing data centers and also underpins compatible public cloud offerings, forming the foundation for the industry's only hybrid cloud model. With the support of more than 3,000 applications from more than 2,000 ISV partners, vSphere is the trusted platform for any application.

Key Benefits of VMware vSphere are:

- Efficiency through utilization and automation – Achieve consolidation ratios of 15:1 or more and improve hardware utilization from 5–15 percent to as much as 80 percent or more—without sacrificing performance.
- Maximize uptime across your cloud infrastructure – Reduce unplanned downtime and eliminate planned downtime for server and storage maintenance.
- Dramatically lower IT costs – Reduce capital expenditures by up to 70 percent and operational expenditures by up to 30 percent to achieve 20–30 percent lower IT infrastructure costs for each application running on vSphere.
- Agility with control – Respond quickly to changing business needs without sacrificing security or control, and deliver zero-touch infrastructure with built-in availability, scalability and performance guarantees for all business-critical applications running on vSphere.
- Freedom of choice – Use a common, standards based platform to leverage existing IT assets alongside next-generation IT services, and enhance vSphere through open APIs with solutions from a global ecosystem of leading technology providers.

Virtual Desktop Infrastructure

VMware Horizon: Extend the power of virtualization from the data center to devices. VMware Horizon delivers virtualized or hosted desktops and applications through a single platform to end users. These desktop and application services—including RDS hosted apps, packaged apps with VMware ThinApp, SaaS apps, and even virtualized apps from Citrix— can all be accessed from one unified workspace across devices, locations, media and connections.

Leveraging complete workspace environment management and optimized for the software– defined data center, Horizon helps IT control, manage and protect all of the Windows resources end users want, at the speed they expect, with the efficiency business demands.

In this new mobile cloud world, managing and delivering services to end users with traditional PC-centric tools has become increasingly difficult. Data loss and image drift are real security and compliance concerns. And organizations are struggling to contain costs. Horizon provides IT with a new streamlined approach to deliver, protect, and manage Windows desktops and applications while containing costs and ensuring that end users can work anytime, anywhere, on any device.

Horizon allows IT to centrally manage images to streamline management, reduce costs, and maintain compliance. With Horizon, virtualized or hosted desktops and applications can be delivered through a single platform to end users.

Desktops and Applications Delivered Through a Single Platform: Deliver virtual or hosted desktops and applications through a single platform to streamline management, easily entitle end users, and quickly deliver desktops and applications to end users across devices and locations.

Horizon provides a single platform for delivering hosted Windows applications and shared desktop sessions from Windows Server instances using Microsoft Remote Desktop Services (RDS), virtual desktops, and ThinApp packaged applications.

Horizon now supports both Windows as well as Linux-based desktops including RHEL, Ubuntu, CentOS and NeoKylin.

Unified Workspace with Secure and Trusted Access: With Horizon 6, IT can support real-time validation, streamline identity management across identity sources like active directory and LDAP, and provide end users with contextual and customizable access to resources through a single unified workspace.

Horizon 6 supports 2-factor, smart card and biometric authentication. It is designed and certified to meet the most demanding compliance regulations including those of the Federal US Government.

Desktops and applications that can be securely delivered and accessed through the unified workspace include:

- Horizon virtual desktops
- XenApp 5.0 and later
- RDS-hosted apps and desktops for Windows Server 2008 and later
- SaaS applications
- ThinApp 5.0 and later
- VMware Horizon Air Desktops and Horizon Air Apps

End users can also use single-sign on (SSO) from their Unified Workspace Web app portal to sign in to AirWatch Web Secure Content Locker and to enroll their devices if they are also using AirWatch Mobile Device Management.

Table 29. VMware IaaS Enablement Catalog

6.1.4 As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of Attachments C & D. {8.1.4}

6.1.4.a Affirmation of Willingness to Comply with the Requirements of Attachment C: NIST Service Models

VMware complies with the requirements of Attachment C: NIST Service models. VMware's broad and deep product offerings span the full gamut of NIST's cloud service delivery models (i.e. IaaS, PaaS, and SaaS) and cloud deployment models (i.e. Public, Private, Community, and Hybrid). Our product offerings have been designed to integrate and interoperate to aid consumers that wish to take advantage of multiple cloud delivery and deployment models.

For example, VMware's public cloud offerings which are sold under the vCloud Air and vCloud Government Service (vCGS) brands, are built upon our industry leading vSphere Hypervisor, our innovative NSX software defined networking platform, and other VMware Technologies.

This design strategy ensures that vCloud Air's virtualization infrastructure is fully compatible with 80% of virtualized data centers deployed today. In context of NASPO, 80% of Participating Entities could benefit from the unique ease of integration of VMware's vCloud Air Services and their existing infrastructure.

As a result, Participating Entities that choose VMware public cloud services will have the unique ability to seamlessly migrate workloads into and out of any of their existing data centers or cloud environments that leverage VMware's vSphere hypervisor as shown in (**Figure 9)** below. A participating entity's VMware-based workloads can be migrated into and back out of vCloud Air at any time, for any reason, without conversion or modification of workload. The same cannot be said for public clouds which are built upon other hypervisors. In the case of other cloud providers, workloads must be converted to run on their hypervisors, and in most case network devices, storage, and other critical infrastructure must be replaced with proprietary equivalents of the participating entity's existing infrastructure. VMware allows Participating Entities to avoid this additional cost and risk, as well as the resulting lock-in.

Participating Entities that wish to leverage VMware's NSX virtual networking technology will also be able to take advantage of VMware's unique Cross-Cloud vMotion capabilities. This capability will allow Participating Entities to us a layer 2 VPN tunnel (**Figure 9**) to extend their existing local area network to VMware's public clouds. As a result, they will be able to move running virtual machines to and from the public cloud in real time with no downtime. This ground breaking capability will enable agencies to:

- **Permanent migrations:** Permanently relocate workloads between clouds.
- **(Planned) Disaster avoidance:** Migration to/from cloud for maintenance and disaster avoidance (weather, etc.).
- **Multi-site load balancing:** Meet regional demand by moving workloads closer to users.
- **Follow the sun:** Move workloads based on time of day to meet global customer demand.

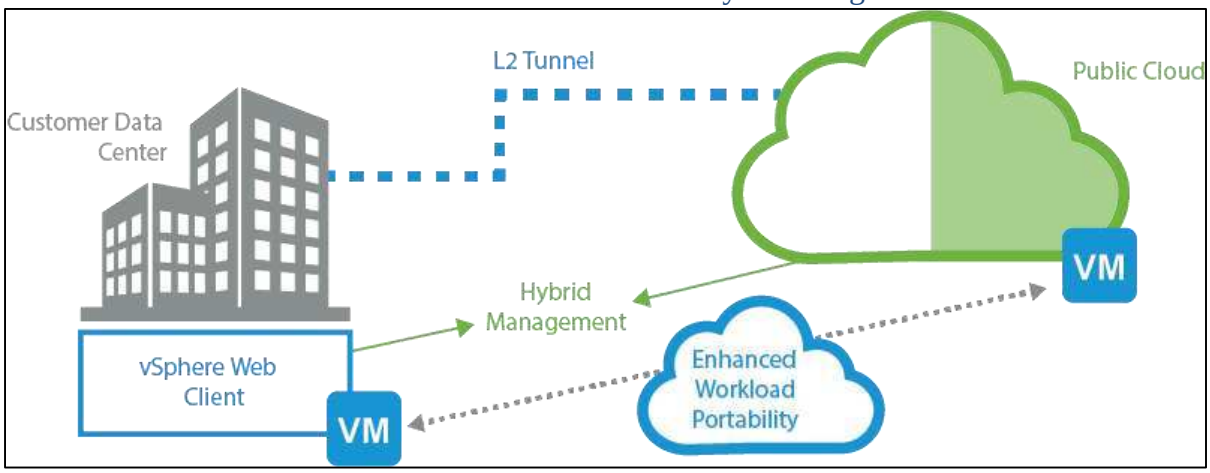


Figure 9. Simplified Migration with VMware Cross-Cloud vMotion

In accordance with RFP Attachment C - NIST Service Models, VMware has organized our service catalog by NIST service model. When we organized our catalog, we took into account guidance provided in Attachment C by ensuring the following recommendations were followed when organizing our service catalog:

- Visibility to the purchasing entities to facilitate simplified matching of requirements to service characteristics.
- The primary focus of each service and avoided classifying services more than once to eliminate duplication within the catalog.
- The most likely consumer of each type of service to ensure that each service was located in the section of the catalog where its target consumer was most likely to look for it.
- The lowest level of configurability for each service to ensure that we had not miscategorized it.

Because our services are traditionally classified along these best practice guidelines, building the catalog was not difficult. We made an effort not to categorize or package our products in a way that differs from our standard offerings, this will ensure that orders are fulfilled using a standard VMware process to avoid any unnecessary delays.

6.1.4.b Affirmation of Willingness to Comply with the Requirements of Attachment D: Scope of Services

VMware, Inc. is a cloud based services provider as defined in section 1.1.1 of Attachment D.

VMware's vCGS offering is FedRamp certified. vCloud Government Services can store and secure both Low Risk Data and Moderate Risk Data as defined by FIPS PUB 199 If a Participating State or Participating Entity requires storage and security of High Risk Data, that could be achieved by enhancing vCGS controls as part of the execution of that State's or Entity's requirements.

Prior to signing a Participating Addendum, VMware and the Participating State will cooperate and determine what type of risk categories of the data are going to be utilized under the Participating Addendum. VMware will provide the appropriate services to meet the requirements of the Participating State.

In addition, all VMware private cloud enablement products included in this proposal (e.g. VMware vSphere, VMware NSX, VMware Virtual SAN, etc.) provide private cloud data centers with the technology needed to meet these requirements on premises.

6.1.5 As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in Attachment D. {8.1.5}

VMware Response:

6.1.5 Adherence of VMware's Offerings to Services, Definitions, and Deployment models identified in RFP Attachment D

An in depth discussion of VMware's offerings' adherence to the services, definitions, and deployment models is provided above in sections 6.1.1-6.1.4 above.

6.2 SUBCONTRACTORS {8.2} (E)

6.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3. {8.2.1}

VMware Response:

VMware intends to provide cloud solutions directly and through the use of subcontractors (or authorized resellers). Subcontractors (or authorized resellers) may be used for product order fulfilment or delivering professional services in accordance with specific orders.

Product Order Fulfilment

When a customer places an order for VMware cloud solutions, they may do so with an authorized reseller that VMware includes under the contract, or directly with VMware.

The authorized resellers are an extension of the VMware sales and engineering teams. They can assist Utah and/or Participating Entities that utilize the contract with the design of the cloud

solution, facilitate order processing, customer invoicing, and payment processing in a streamlined manner and can provide professional services if required by the customer.

- The authorized resellers that VMware selects for this contract must meet the Administrative, Business and Technical Requirements of the final RFP as well as maintain an active reseller agreement with VMware and be certified to sell and implement VMware cloud solutions.

Additional criteria that VMware considers, but does not require, when selecting authorized resellers includes:

- Maintaining a local office(s) in the Participating Entities' state,
- Qualifying as a small, disadvantaged, women owned, or minority business,
- Reviewing the number of public sector pre sales and engineering staff that are assigned to support the contract, and
- Agreeing to a sales and marketing plan with VMware to help promote VMware cloud solutions and the NASPO Cloud Contract.

VMware works diligently with its resellers to maintain VMware product and corporate knowledge as evidenced through a rigorous certification process. This knowledge is maintained through ongoing trainings and recertification. Whether fulfilling an order directly with VMware, or through an authorized reseller, customers can expect the same level of service for the cloud solutions that are delivered.

Delivery of Professional Services

VMware may decide to use subcontractors for any VMware primed engagements for professional services. Our intent is to staff engagement(s) with VMware full time equivalent (FTE) resources first. If no VMware FTE resources are available with specific skills, required location, or ability to support the duration of the engagement, then we engage resources from our authorized reseller/preferred partner list. VMware affirms that it assumes full accountability and responsibility for the completion of the contracted work with the end customer.

6.2.2 Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement. {8.2.2}

VMware Response:

VMware's use of subcontractors under the contract may occur under the following scenarios:

Delivery of Professional Services

VMware may decide to use subcontractors for any VMware primed engagements. Our intent is to staff the engagement(s) with VMware full time equivalent (FTE) resources first. If no VMware FTE resources are available with specific skills, required location, or able to support the duration of the engagement, then we engage resources from our preferred partner / vendor list. VMware still assumes full accountability and responsibility for the completion of the contracted work with the end customer.

Authorized Resellers for Fulfilment

VMware's business model is designed to sell our products and cloud services through a network of authorized resellers. To maximize sales and marketing efforts under the contemplated contract, support local in-state and small businesses resellers, and provide customers with flexibility to work with an authorized reseller of their choice, VMware will be using authorized resellers for product fulfilment under the contract.

Under the contemplated contract, authorized resellers will work with the end customer on the following items: creation of technology design, required bill of material, ordering of VMware products, invoicing and payment, and installation service if they are required.

Table 30 below provides the estimated usage of subcontractors / resellers for orders processed under the resulting contract.

Entity	Professional Services	Fulfilment of Product / Cloud Services
VMware, Inc.	80%	5%
Subcontractors / Resellers	20%	95%

Table 30. Percentage of work performed between VMware and subcontractors / resellers.

Please refer to VMware's Sales and Marketing Plan located in **Appendix E** for more information on the authorized resellers VMware intends to use under the resulting contract. In addition, the names, office locations, and size of sales and engineering staffs for each VMware authorized reseller is provided in section 6.2.3 below.

6.2.3 If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP. Include a description of how the Offeror will ensure that all subcontractors and their employees will meet all Statement of Work requirements. {8.2.3}

VMware Response:

Our initial list of subcontractors (authorized resellers) that we intend to utilize under the contract is provided in **Table 31** below. In addition to their in-state presence, presales and engineering support, the qualifications for each subcontractor / reseller includes:

- Maintaining an active reseller agreement with VMware;
- Certification to sell VMware cloud service offered under the contract;
- Agreement, in writing, to accept the terms, conditions and requirements that VMware agrees to under the master contract with Utah and any Participating Addendum with a Participating Entity (this ensures contract compliance from subcontractors / resellers);
- Participation in VMware-led training, which includes a review the contractual obligations for resellers / subcontractors; and
- Annual recertification of all requirements of the contract are maintained.

Managing Requirements for Subcontractor and Resellers

VMware has amended its authorized reseller on-boarding process to include a check list of NASPO RFP requirements. Resellers and/or subcontractors will be required to meet or exceed all NASPO requirements to enter into and/or maintain a master agreement with VMware. If the reseller / subcontractor meets these criteria and is approved by the Lead State, the reseller / subcontractor will be required to complete a reseller agreement rider from VMware that flows the master contract terms (and Participating Addendum terms). Lastly, as part of VMware's annual recertification to the Lead State, we will conduct a follow up questionnaire and requirements check in writing from all resellers / subcontractors to ensure ongoing contractual compliance.

Reseller Name	States w/ Offices	# Sales Executives Supporting State / Local Govt. / Education	# Engineers Supporting State / Local Govt. / Education
Advanced Network Management	CO, NM	12	20
Advanced Systems Group	CO, ID, MT, UT, WA	12	11
Advizex	CT, MA, ME, NH, RI, VT	14	24
Alexander Open Systems	MO	15	18
Atrion	RI	14	7
CDI	NJ	6	15
Compunet	ID, OR, WA	8	5
Dimension Data	CA	10	8
Dyntek	NJ	16	4
En Pointe/PCMG	CA, HI	11	10
Enterprise Networking Solutions	CA	5	8
ePlus	CA, CT, MA, ME, NH, NV, RI, VT	18	26
GKR Systems, Inc. dba Venture Technologies	MS, TN	14	14
GovC	NH	4	2
Insight Public Sector, Inc.	AZ, CA, FL, GA, IL, KS, MA, MN, NY, OH, TX, VA, WA	25	18
ISC, Inc. dba Venture Technologies	CO, MT, NM, UT	9	24
Ivoxy	OR, WA	4	6
Kovarus	CA, NV	7	15
MicroAge	AZ, CA, FL, GA, IL, KS, MA, MN, NY, OH, TX, VA, WA	5	3
NWN	CA	10	15
PEAK Resources, Inc.	CO	8	12
Presidio	CT, MA, ME, NH, RI, VT	20	27
Promedia	NJ	9	4
Solutions II	CO, NV, UT, WA	13	11
World Wide Technologies	WA, CA, AZ, NM, CO, IL, TX, TN, FL, NC, VA, NJ, NY	8	15
Zones	OR, WA	25	3
	Total	**302**	**325**

Table 31. Listing of proposed VMware subcontractors / reseller

6.3 WORKING WITH PURCHASING ENTITIES –{8.3} (E)

Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

- Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;
- Response times;
- Processes and timelines;
- Methods of communication and assistance; and
- Other information vital to understanding the service you provide.{8.3.1}

VMware Response:

6.3.1.a Data Breach Monitoring and Notification

If VMware determines that there has been unauthorized access to, use of, or disclosure of customer content, VMware will use commercially reasonable efforts to notify customers taking into account any applicable law, regulation, or governmental request. This notification and subsequent follow-up will be done by and in coordination with the contract manager and support team identified in in our response to RFP section 7.1 which is found in section 5.1 of this document.

6.3.1.b Personnel, Process, Timelines, and Methods of Communication and Assistance

The following is a notional outline of VMware's Data Breach Response Plan. The official documented VMware data breach response plan is proprietary and confidential, but the following best practice approach provides a high level summary of the plan to demonstrate that it is in alignment with industry and Government best practices.

6.3.1.c Prior to a Breach

Preparedness is critically important to the defense of data in the cloud. VMware has prepared by producing a data breach response plan to ensure that the proper processes are followed before, during, and after a breach. This plan is maintained by our information assurance teams and is regularly reviewed and updated by a multi-disciplinary data breach response team comprised of individuals from VMware's security, compliance, engineering, and leadership teams. Personnel are trained on defined Incident Response roles and responsibilities according to NIST SP 800-53.

Prior to and during a data breach, VMware's Security Operations Center (VMware vCloud Air) or Carpathia's Security Operations Center actively monitors its vCGS infrastructure for intrusions.

6.3.1.d During and After a Breach

In the event of a security breach, VMware follows a proprietary process that is outlined in our data breach response plan. To aid in evaluation of this response, we provide a non-proprietary, high-level summary of our process below in **Table 32**:

Step	Notional Activity Summary
1	Discover the Breach via both manual monitoring and automated tools.
2	Lock down the systems in question by revoking access privileges for all but a specialized response team and removing systems from external networks.
3	Investigate the extent of the breach to determine to what extent countermeasures (Intrusion Prevention Systems, firewalls, etc.) have been successful, and what data has been compromised or lost.
4	Remediate by (1) re-establishing the security perimeter with new credentials, (2) establishing necessary credentials using a whitelist approach to allow only critical personnel access, (3) Restoring servers and data from backup and run signature analysis to ensure that no malware is present, (4) once the root cause vulnerability(ies) have been identified and eliminated, only then will we restore network connectivity to the systems.
5	Activate the VMware data breach response team (including the NASPO contract manager) to manage the situation going forward.
6	Notify the authorities if applicable and necessary.
7	Bring in specialized support. Where necessary, VMware will utilize internal external forensics experts, attorneys, etc. to determine the full scope of the data breach and to ensure that no further damage is done to our clients or VMware.

Step	Notional Activity Summary
8	Determine whether identity protection is required. In the event of loss of personally identifiable information or other highly sensitive data VMware will work with effected parties to determine whether Identity theft protection services are warranted, etc.
9	Establish communication channels to the public. In the event of a large scale breach, a web site would be established and notification would be provided to end users. Mail and email notification would also be employed. VMware's NASPO contract manager would serve as a single point of contact for Participating Entities.
10	Inquiry response. Support staff including the NASPO contract manager would be notified of all information required to handle user inquiries.
11	Return to nominal operation.

Table 32. Estimated Data Breach Response Plan

Our comprehensive certifications such as FedRamp are evidence that VMware meets the requirement for maintaining a data breach management processes.

6.3.1.e Response time

Notification timeframes are agreed upon between VMware and the customer in standard agreements and contracts. Incidents are handled on a case-by-case basis, but typically occur between 24-48 hours after a breach has been confirmed.

6.3.2 Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement. {8.3.2}

VMware Response:

VMware will ensure that its NASPO program management plan, policies, procedures, and subcontracting/reseller agreements prohibit VMware employees and agents (resellers) from pushing adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement. VMware will emphasize this point during the mandatory training to all resellers that are authorized under our contract.

6.3.3 Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production. {8.3.3}

VMware Response:

VMware IaaS Services

VMware vCloud Air

VMware offers free production services for the purpose of trails, user testing, and staging for new customers. Details of these offers are below in **Table 33**.

vCloud Air Service	Trial Offer
vCloud air Virtual Private Cloud	VMware offers a variety of testing and training periods with its service offerings. Trials and testing periods can be arranged for a 30-day period. For additional detail, see section 6.18 below.
vCloud Air OnDemand	Get $300 in service credits for your first 90 days when you sign up for our pay-as-you-go public cloud. Virtual Private Cloud OnDemand lets you stand up new

vCloud Air Service	Trial Offer
	infrastructure in minutes, with no up-front resource, size, capacity, or cost commitments.
vCloud Air Dedicated Cloud	VMware offers a variety of testing and training periods with its service offerings. Trials and testing periods can be arranged for a 30-day period.
vCloud Air Object Storage	Get $300 in service credits for vCloud Air Object Storage powered by Google Cloud Platform when you sign up for vCloud Air OnDemand. Get instant, self-service access to storage capacity, and store and retrieve your data with high levels of durability and performance.
vCloud Air Disaster Recovery	VMware offers a variety of testing and training periods with its service offerings. Trials and testing periods can be arranged for a 30-day period.

Table 33. VMware Trial Offers

Beyond the stated free trials, the vCloud Air business unit will work with Participating Entities to assess and complete additional proof of concept engagements and tests as required for their requirements and orders.

VMware vCGS

Resources can be made available in support of vCGS proof of concepts and trials subject to mutually agreed upon business justification, scope, and resource availability.

VMware AirWatch

- AirWatch provides a free trial environment that is identical to production. AirWatch encourages the use of our free trial as part of customer acceptance strategy
- Our free trial enables you to review all solution functionality
- Enroll any of the device types we support, including, Android, Apple, Windows and BlackBerry
- Access the complete feature set and leverage our full array of web APIs
- Explore trial guides and live training webinars
- Use our expansive customer tools and resources

AirWatch also offers Testing upgrades. We offer two options for user acceptance testing (UAT): a “sandbox” environment and a dedicated environment

- UAT Sandbox – Create individual or combined sandboxes for UAT users within a single AirWatch environment, leveraging the multitenancy of the solution
- UAT Environment – Create a new cloud environment solely for UAT, independent of the production environment and using dedicated hardware and software
- UAT sandboxes and environments are scoped and priced separately

6.3.4 Offeror must describe whether or not its computer applications and Web sites are be accessible to people with disabilities, and must comply with Participating entity accessibility policies and the Americans with Disability Act, as applicable. {8.3.4}

VMware Response:

VMware is dedicated to making its products and technologies accessible to people with disabilities. We provide more than 170 voluntary product accessibility templates (VPAT) on our publically available accessibility website. The VPAT is a document which evaluates accessibility of a particular product according to standards set forth in the Section 508 amendment of the United States Rehabilitation Act of 1976. It is a voluntary vendor-disclosed document which details each aspect of the Section 508 requirements and how the product supports each criteria.

VMware's computer applications and Web sites are accessible to people with disabilities in accordance with applicable federal, state and local laws. VMware will comply with Participating Entity's accessibility policies and the Americans with Disability Act, as applicable and as finally negotiated between the Purchasing Entities through its Participating Addendum.

VMware AirWatch

The AirWatch console is available through major browsers for simplified administration of the entire device fleet; AirWatch enables secure mobile access to enterprise resources on enrolled devices. Additionally, our solution runs on Microsoft products such as Microsoft SQL Server and Internet Explorer to help bolster accessibility.

- We offer a broad range of functionality in our product and for this reason it is a challenge to attain full compliance with accessibility standards. Our development and UI teams follow best practices when designing our software solutions and we will continue to work with our customer and partner communities to meet relevant accessibility needs where possible.

6.3.5 Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at minimum. {8.3.5}

VMware Response:

VMware IaaS Services

At the time of its response, VMware vCloud Air and vCGS applications and content delivered through Web browsers are accessible using current released versions of multiple browser platforms. The following browsers are supported in the vCloud Air and vCGS consoles.

- Internet Explorer 8 and later
- Firefox 3.6 and later
- Safari 4 and later
- Chrome 10 and later

VMware anticipates compliance with commercially available web browsers as they are updated and changed over the term contemplated by the Master Agreement but respectfully reserves the right to either certify or adjust this statement for unknown terms in the future, through the annual recertification process outlined in RFP CH16012.

VMware AirWatch

Administrators can access the software from any web browser, anywhere in the world by simply logging into our web-based console. The software does not need to be downloaded, installed or configured.

- AirWatch recommends using the latest version of the following compatible browsers:
- Internet Explorer
- Firefox
- Safari
- Google Chrome
- The console may also be compatible with other browsers, such as Opera, that are not officially certified

6.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations. {8.3.6}

VMware Response:

VMware IaaS Services

VMware will meet with the Purchasing Entity and hold a meeting to determine whether any sensitive or personal information will be stored or used in the Service that is subject to any applicable law, rule or regulation providing for specific compliance obligations.

Once awarded, we will implement a sales & marketing plan which will include outreach to Participating Entities to let them know we are interested in negotiating a Participating Addendum and setting up a meeting to discuss their sensitive info storage needs/storage requirements. We will determine the sensitivity level of their document using FIPS publication 199 as guidance. We will also identify any specific compliance requirements the agency must meet such as CJIS, HIPAA, etc. VMware will work with the Participating Entity to provide a solution and service to meet their specific needs.

VMware AirWatch

By default, the solution only collects information necessary to manage the device, such as the device status, compliance information, OS, etc.; our solution may collect (if configured by administrator) or users may input data considered to be sensitive. Customers can use privacy controls to limit the collection and/or display of data.

- AirWatch defines customer data related to the solution and/or hosted service as follows:
- Customer Content – any and all data, applications, files, information or materials accessed, transmitted, uploaded, published or displayed through the software or hosted service by you, your users or any third party users and/or their devices. It does not include relationship data or usage data.
- Customer Personal Data – personally identifiable information from or about an individual either provided by customer or customer's users or a device to VMware in connection with your use of the software or hosted service. Personal data does not include information relationship data or usage data or anonymous or non-identifying data.

- Relationship Data – Personal information that VMware collects during the activation and maintenance of your account. It may include names and contact details of your personnel involved in maintaining the software and/or hosted service. It does not include information collected through the publicly accessible portions of our webpages, which is subject to the privacy policy posted on those webpages.
- Usage Data – Aggregated technical data about your use and your users' use of the software and/or hosted services and your user's devices
- Applicable data at rest and data in transit are encrypted using strong encryption algorithms to help ensure data integrity.

6.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers. {8.3.7}

VMware Response:

If a customer is using VMware Professional Services to assist with the implementation of cloud solutions, they follow a detailed process for the implementation of the service. As part of the service, a detailed schedule is created with input from the client to outline the requirements for configuration, implementation, testing, and training for the project. Depending on the size and scale of the implementation, the timeline can vary greatly. Provided in **Figure 10** below is a sample high-level schedule for an engagement.

Estimated Schedule and Working Hours

VMware estimates that this entire project will not exceed thirteen (13) calendar weeks to execute if all assumptions in End Customer Responsibilities and Assumptions section are met and there are no intervening delays outside of VMware control. Work will be performed according to a schedule agreed upon by both parties. Typically, work is performed during normal business hours and workdays (weekdays and non-holidays).

The estimated duration for each of the project phases and programs is as follows:

- Project Kickoff – 1 week
- Phase 1
  - Management Program – 8 weeks
  - Security Program – 4 weeks
- Phase 2
  - IaaS Program – 7 Weeks

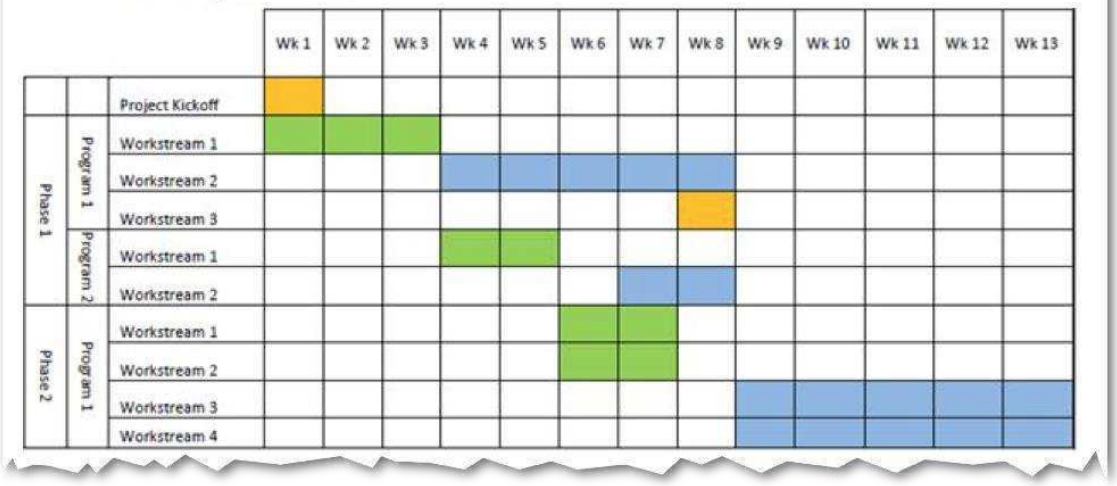


Figure 10. High-Level Implementation Schedule

6.4 CUSTOMER SERVICE {8.4} (E)

Offeror must describe how it ensure excellent customer service is provided to Purchasing Entities. Include:

- Quality assurance measures;
- Escalation plan for addressing problems and/or complaints; and
- Service Level Agreement (SLA). {8.4.1.}

Quality Assurance Measures

VMware's vCloud Air and vCGS operations staff follow ITILv3 best practices for strategy, design, transition, operations, and continual service improvement. From a service operations standpoint, all incident, event, problem, change, release, and configuration management processes are based upon ITILv3 standards.

VMware vCloud Air has achieved ISO/ IEC 27001:2005 Certification of its Information Security Management System and has completed SOC II Type 1, SSAE 16 SOC 1 Type II and SOC 2 Type II examinations.

Escalation Plan

The VMware Contract Manager (CM) is the primary point of contact for all aspects of the contract, including the escalation of any problems and/or complaints. The CM will work with the extended VMware team to manage all aspects of the contract. A summary of the internal teams that the CM will interface with to manage the contract is provided in **Figure 11** below. This summary includes escalation and resolution of any issues that may arise.

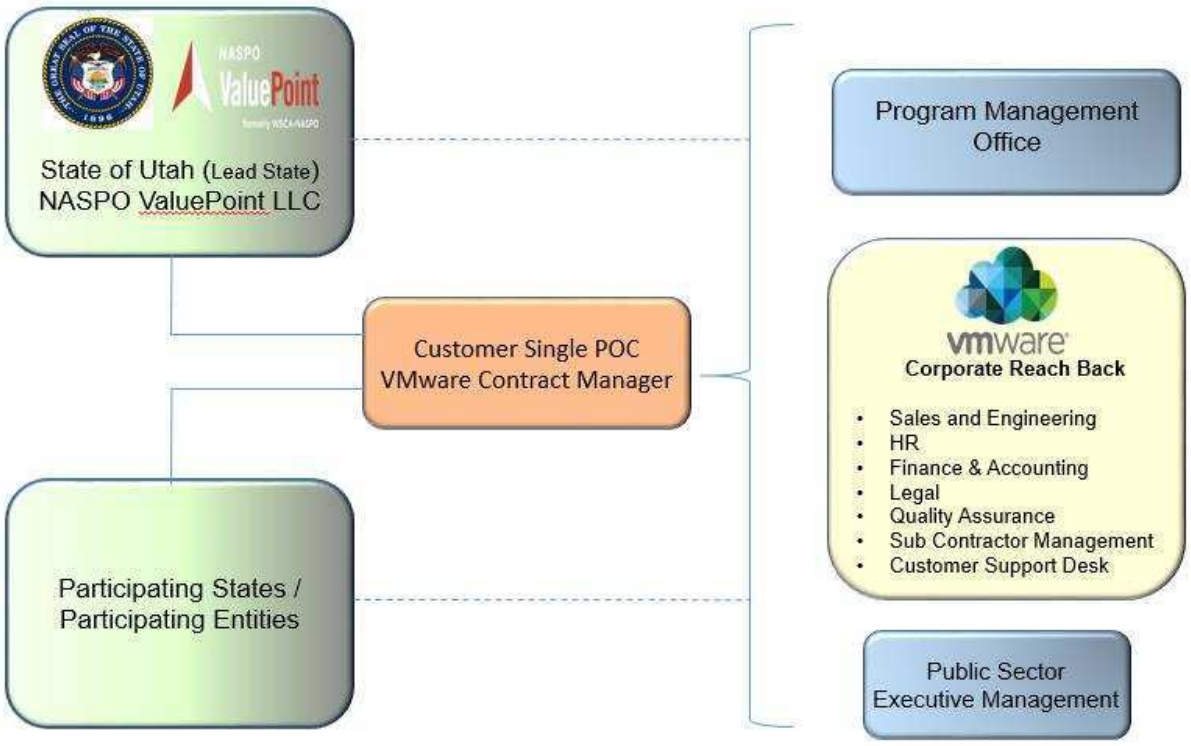


Figure 11. VMware's Escalation Management Plan

Our standard escalation plan, specific to VMware IaaS cloud services, is outlined below. This plan is also available for troubleshooting problems should they arise. End customers can contact the Contract and Delivery Managers identified in this proposal response section 5.1 in addition to the standard support options provided in the following support request explanations.

How to Escalate a Support Request

Your VMware support team will ensure that the appropriate resources are committed to fulfilling the requests of Participating Entities to ensure a timely resolution. If Participating Entities are not satisfied with the progress of support request resolution, they can request an escalation. By invoking the escalation process, additional levels of VMware management attention, procedure reinforcement and resource prioritization are brought to bear on resolving the support request. We do not anticipate a need for such escalation, however, in the event that escalation is necessary, the following process should be followed by the Participating Entity.

When to escalate a support request

- Your production system goes down during an upgrade or other implementation
- You need to communicate a critical business impact to VMware Support Management
- You are dissatisfied with the responsiveness to or resolution of a support request

Escalation Steps

- First, The Participating entity should review the details of the delayed support request and verify the following facts:
  - Is the problem statement correct?
  - Does the support request accurately describe the business impact?
  - If there is a workaround, is it impractical or inappropriate?
  - Is there a critical milestone date identified in the support request?
- If it is determined that an escalation is required, the Participating Entity should call VMware Support at 1-877-486-9273.
- Ask that the existing Support Request (SR) be escalated. The technician assigned to the SR, their manager, or the current Duty Manager will escalate the SR.

Once a request is escalated

Once an escalation request has been made, the appropriate Regional Escalation Manager will evaluate the situation to identify the process corrections to make or the appropriate resources to assign. An Escalation Engineer that specializes in the type of situation being experienced will be assigned as the primary point of contact for the issue and will coordinate with all parties involved to ensure an expedited resolution.

The Escalation Engineer will set up a conference call with the appropriate parties to begin outlining the action plan and troubleshooting the situation. The Regional Escalation Manager is made aware of all escalations and their current status on a daily basis. The Regional Escalation Manager will work with the primary Escalation Engineers to ensure that the appropriate resources, communication and action plans are in place to expedite resolution. **Figure 12** below provides a flow chart of the standard escalation process.

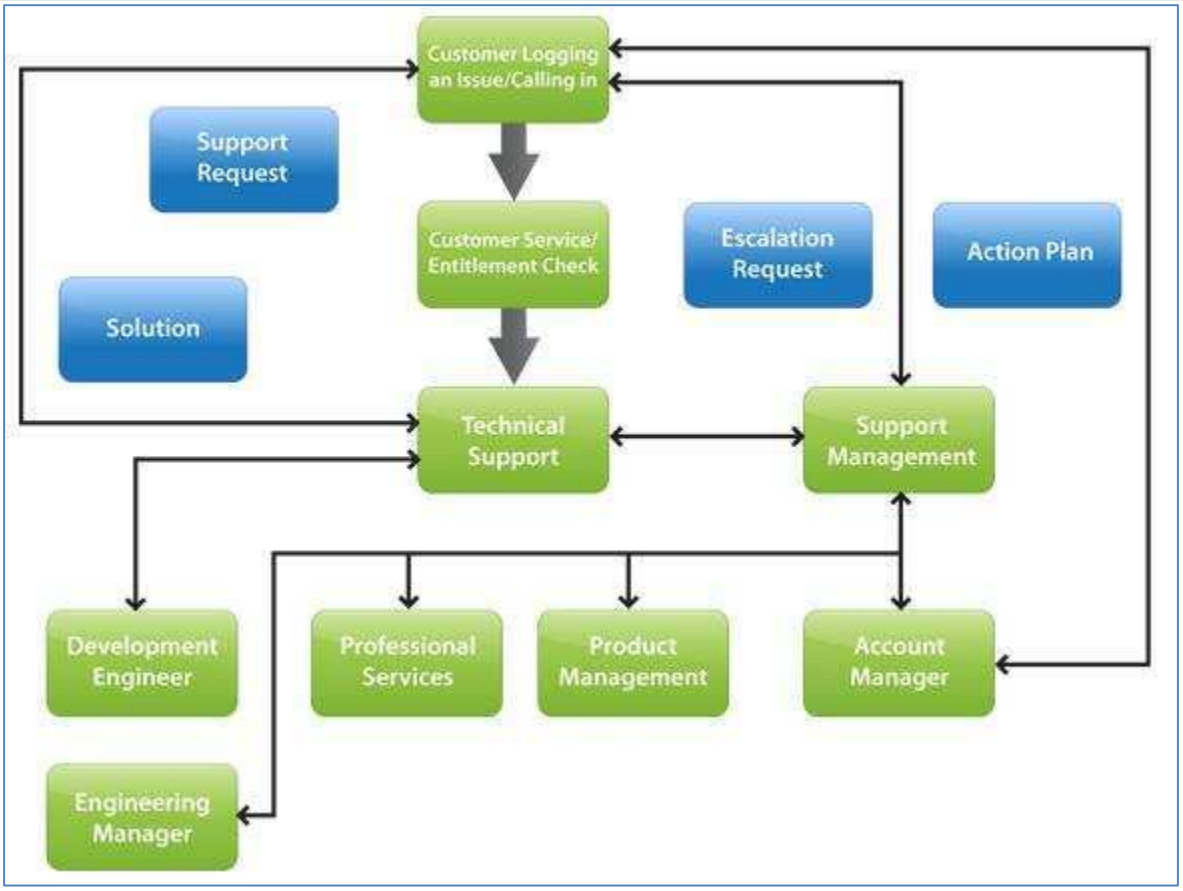


Figure 12. VMware's IaaS Escalation Plan

AirWatch Support and Escalation

AirWatch provides Enterprise Support Services designed for our top-tier customers that covers multiple products and unlimited licenses at a fixed cost. With seven global support centers and support provided in 18 languages, customers have access to 24/7/365 worldwide support with unlimited incidents, expedited level two technical expertise and dedicated technical account management. This includes a dedicated support line providing immediate access to an AirWatch representative.

Participating Entities may opt for a dedicated Technical Account Manager (TAM), for an additional cost. If they do so, calls are routed during business hours to their dedicated TAM. During off-hours or in the unlikely event that the TAM is unavailable, the call will route to Tier two technical expertise.

Pre-Implementation

A dedicated Account Executive will assess requirements, provide education on options, demonstrate capabilities and assist with other project needs.

- Participating Entities will receive a comprehensive "How-To" package via email that outlines the required pre-installation steps and includes checklists, worksheets and instructional documentation.

- The Participating Entity's Account Executive and implementation consultant will schedule and conduct pre-installation meetings to ensure all pre-requisites are complete before the implementation.

Implementation and Design

Implementing AirWatch is a streamlined process due to our solution's inherent design, our highly defined implementation methodology and an implementation team that is prepared to guide our customers and partners through the deployment process. The Participating Entity's dedicated implementation consultant will:

- Serve as your main point of contact for all implementation activity and will coordinate other internal resources as necessary. The consultant can communicate with your resources as appropriate based on your project structure.
- Manage the overall project timeline and process, using a proven process we have used successfully to implement more than 16,000 customers.
- Interface directly with you and other team members to support the day-to-day tasks involved with the implementation of the solution including: customer assessment, system configuration, testing, training, and troubleshooting/issues resolution.

Implementation is complete once all deliverables have been met and the customer is successfully transitioned to the support team.

Post-Implementation

We are dedicated to providing each customer with opportunities to interact with our team when a technical question or incident may arise. Our global support offering provides customers with access to the myAirWatch Portal and global Support Services.

- The myAirWatch Portal provides 24/7/365 access to AirWatch resources such as installation and product documents, FAQs, interactive community forums, pre-recorded webinars and AirWatch Academy training resources.
- The AirWatch Support Portal (located in myAirWatch) enables customers to create new support requests and update or track the progress of any open tickets. This feature includes visibility into Support staff feedback, solutions, and ticketing history.
- Get the level of Global Support Services that is appropriate for your program, with 24/7/365 coverage for Severity 1 incidents and unlimited online support requests for all support levels.
- AirWatch offers a full array of optional professional services to support businesses with requirements that go beyond implementation services. Our technical experts are prepared to help you assess technology needs and will provide on-site training, mobility best practices, integration services and technical solutions to improve business processes and reduce operational costs. Businesses using our services benefit from the company's deep domain expertise and experience in building, implementing and scaling enterprise software solutions.

Service Level Agreements

Please refer to **Appendix C** of our response for the full description of VMware's SLAs.

6.4.2 Offeror must describe its ability to comply with the following customer service requirements: {8.4.2}

VMware Response:

VMware agrees to comply with the customer service requirements outlined in the RFP and is prepared to do so as described in the sections below.

6.4.2.a You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current. {8.4.2.a}

VMware Response:

We have identified a single point of contact, identified in this proposal response section 5.1 with contact information available to Participating Entities. The Contract Manager identified in section 5.1 is also the designated, lead representative to manage the negotiations for each Participating Addendum, and will also maintain current contact information for the term of the contract. Participating Addendum negotiations will involve input from various internal departments which will be coordinated through the lead representative.

6.4.2.b Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones. {8.4.2.b}

VMware Response:

Our VMware Support Department is our designated point of contact for technical customer service inquiries. These representatives are accessible by phone at 1-877-486-9273 or via email 24 hours a day / 7 days a week.

6.4.2.c Customer Service Representative will respond to inquiries within one business day. {8.4.2.c}

VMware Response:

VMware customer Services Representatives will respond to inquiries within one business day or sooner.

6.4.2.d You must provide design services for the applicable categories. {8.4.2.d}

VMware Response:

We have provided a summary of our design and installation services in Section 6.4, Customer Service. Please refer to this section for a complete service description.

6.4.2.e You must provide Installation Services for the applicable categories.{8.4.2.e}

VMware Response:

We have provided a summary of our design and installation services in Section 6.4, Customer Service. Please refer to this section for a complete service description.

6.5 SECURITY OF INFORMATION {8.5} (E)

6.5.1 Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services. {8.5.1}

VMware Response:

VMware IaaS Services

vCloud Air has logically separated networks that restrict Tenant access to only their own private networks. vCloud Air has two offerings: (1) The Dedicated Cloud option provides physically isolated and reserved compute resources from all other vCloud Air tenants, as well as a private cloud instance and (2) the Virtual Private Cloud option has a multitenant compute resource mode. Both services have logically isolated networking and storage that ensures secure resource separation. Customers have complete control over the file systems and databases they deploy within the service.

VMware security teams perform OSINT monitoring on the Internet for all of our products and services. This includes harvesting data from search engines, file sharing, and social networking sites. This data is analyzed for keywords and other specific indicators. With regards to potential data leaks, the customer is solely responsible for protecting the security of your content, including any access provided to employees, customers or third parties. The vCloud Air provides certain software and functionality to help protect content from unauthorized access such as firewalls, load balancers, IPSec VPNs. You may deploy additional capability to address other security controls such as data encryption, intrusion detection, file integrity monitoring, etc.

We do not monitor customer environments for security threats or attacks, it is up to the customer to protect their tenant VM environments. VMware does monitor security tools for effectiveness, applicability, and ensure they are up-to-date on routine basis to ensure all controls are at their optimum capacity. However, this information is not shared with customers to maintain the operational security of the environment, nor can we allow customers to perform testing against the management infrastructure due to the potential for a customer to affect another customer's experience. VMware performs regular vulnerability and penetration testing on the management infrastructure to ensure all controls are effective and secure. Effectiveness of security controls can be reviewed within the independent third party audit reports.

VMware's Data Destruction policy outlines the following: The proper disposal of information system assets is a key factor in maintaining data security. All media containing VMware data shall be removed from decommissioned assets and secured before the asset is destroyed, donated, or otherwise disposed of by the Company. The removed media shall be sanitized before being recycled or destroyed. Several types of sanitization methods may be employed when decommissioning company-owned assets containing storage media with classified information.

- Disposal – Discarding media with no other sanitization considerations. This is most often done by paper recycling containing non-confidential information but may also include other media.
- Clear/Wipe – A level of media sanitization that protects the confidentiality of information against an attack that can be carried out from the operating system itself or by performing digital forensics on storage media. Simple deletion of items would not suffice for clearing. Clearing (aka wiping) must not allow information to be retrieved by data, disk, or file recovery utilities. It must be resistant to keystroke recovery attempts executed from standard input.
- Destroy – Destruction of electronic or hard copy media is the ultimate form of sanitization. After media are destroyed, it cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting.

VMware AirWatch

Data security is a top priority and AirWatch ensures that multiple logical, physical and administrative controls secure customer data, including encryption for applicable data at rest and in transmission, 24/7 on-site security and CCTV monitoring, and defined Information Security policies.

At the end of the contract, AirWatch can assist the customer in using solution controls to export data. Customers in a Dedicated Cloud deployment can leverage a robust datamart. Data is secured in transmission.

- AirWatch has defined data retention and data disposal policies to safeguard data throughout its lifecycle.

6.5.2 Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security. {8.5.2}

VMware Response:

VMware IaaS Services

VMware vCloud Air has achieved ISO/ IEC 27001:2005 Certification of its Information Security Management System and has completed SOC II Type 1, SSAE 16 SOC 1 Type II and SOC 2 Type II examinations. VMware has also completed an examination of vCloud Air against applicable controls of HIPAA/HITECH and offers a Business Associate Agreement (BAA) to all interested customers using our US-based data centers. These ISO, SOC and HIPAA/HITECH examinations were completed by Brightline CPAs and Associates – an ANAB accredited certification body. vCloud Air is also Safe Harbor certified to meet European Data Privacy compliance regulations.

VMware vCloud Air provides infrastructure as a service to its clients. We do not access or store any client data unless explicitly contracted to do so by the client (e.g., for Disaster Recovery or Data Protection Services). Customers are solely responsible for their own 'Content'. Customer access is restricted to that content and data. Customers do not have the ability to view content from any other customer using the service, and the service is architected from the ground up with this principle in mind. VMware accesses and uses this 'Content' only as necessary to provide the

Service Offering (which we may do with the assistance of affiliates, service providers and contractors), perform or enforce contractual obligations, or comply with applicable law.

VMware AirWatch

AirWatch agrees to comply with applicable laws and regulations in the locations where we do business. Customers are responsible for utilizing our solution in compliance with relevant laws and regulations.

By default, the solution only collects information necessary to manage the device, such as the device status, compliance information, OS, etc.

Users may configure privacy settings to enable/disable the capture of transaction history from enrolled devices, including phone, data and SMS.

6.5.3 Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement. {8.5.3}

VMware Response:

VMware IaaS Services

VMware does not have administrative level access to customer data, operating systems, or access into a customers configured networks. VMware's access control, separation of duty, and other policies define which individuals are allowed to have access to vCloud Air management systems.

VMware AirWatch

Our support staff do not access customer data without customer permission. Environments are accessed by AirWatch administrative staff for maintenance and support purposes only.

All access privileges are technically enforced using role-based access control, the separation of duties, and the principle of least privilege.

6.6 PRIVACY AND SECURITY {8.6} (E)

6.6.1 Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in Attachment D, including supporting the different types of data that you may receive. {8.6.1}

VMware Response:

6.6.1 Compliance with NIST SP 800-145 and Other Relevant Standards

VMware IaaS Services

VMware's proposed cloud solutions are compliant with NIST 800-145 and other relevant industry standards including FedRAMP, FISMA, PCI, CSA CAIQ, etc. Our commitment to compliance is demonstrated by VMware's track record of pursuing and obtaining certifications such as those listed above.

vCloud Government Service has been certified to store and secure Low Risk Level and Moderate Risk Level data as defined by FIPS PUB 199. In addition, VMware is capable of enhancing the vCloud Government Service to meet participating State's requirements to be able to store data that is defined by FIPS Pub 199 as High Risk Data.

VMware is committed to maintaining compliance with all of our existing compliance certifications and to pursue future, applicable certifications as they are updated or created. Our ability to remain competitive as a software and services provider in the public sector depends upon it. Thus we have established a comprehensive security and compliance team to ensure that we maintain compliance as well as a strong security posture.

VMware supports regular internal and external audits to ensure compliance with its certifications as required.

The following are additional ways in which VMware invests in maintaining compliance and security:

- VMware has an Information Security team responsible for securing VMware cloud services, setting security standards and policy, and the deployment and implementation of new security technologies.
- VMware has a dedicated 24/7/365 Security Operations team that is responsible for monitoring VMware cloud services. They perform incident response, forensic investigations, and OSINT monitoring. They also ensure adherence to internal policies and standards.
- VMware has a product security team responsible for evaluating VMware software and products for vulnerabilities. They work closely with R&D and engineering teams to ensure secure coding practices and publish security-related advisories.
- VMware maintains multiple security teams responsible for different aspects of delivering both products and services and maintaining compliance, as well as protecting VMware corporate networks.
- VMware has a dedicated Security Product Line Manager responsible for ensuring adequate security controls and features within the VMware Service offering.
- VMware security teams hold multiple certifications from ISC2, GIAC, as well as others relevant for their particular areas of expertise and focus.
- Several VMware security team members also hold security clearances with the Department of Defense, and are members of other organizations such as the FBI Infragard program and the HTCIA.
- All VMware employees participate in continuing education, training, and certification.
- VMware performs background checks on all new hires. This includes verifying SSN, deemed export control/DPL, education, employment, as well as criminal history.

VMware AirWatch

The AirWatch Information Security Program is built on the security framework laid out in NIST 800-145.

Although AirWatch is not required to register with any regulatory agencies, we provide a suite of tools for our customer's to maintain industry-relevant compliance guidelines within their mobile device fleets. AirWatch has recently been awarded the HP-IAPP Privacy Innovation Award for Most Innovative Privacy Technology by the International Association of Privacy Professionals

(IAPP) for our commitment to delivering an EMM platform focused on end-user privacy. To help ensure the confidentiality, integrity, and availability of our cloud offering, we comply with the European Data Protection Directive (95/46/EC) and our top-tier data center partners have undergone SSAE16 SOC2 Type II audits and have ISO 27001 certifications.

6.6.2 Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply. {8.6.2}

VMware Response:

6.6.2 VMware's Government or Standards Organization Security Certifications

VMware IaaS Services

ISO/IEC 27001: ISO/IEC 27001 is a globally recognized standard for the establishment and certification of an information security management system (ISMS). vCloud Air continues to maintain a current ISO/IEC 27001 Certification and has recently issued updated certification for ISO/IEC 27001:2013. Achieving certification means that VMware has implemented a holistic security program that conforms to the ISO 27001 standard requirements, both in the security management system and control activities. The audit of the ISMS was completed by Brightline CPAs and Associates - an ANAB accredited certification body.

HIPAA: The Health Insurance Portability and Accountability Act of 1996(HIPAA), which has incorporated requirements from the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, established national standards for the security and privacy of Protected Health Information (PHI) in the United States. To help customers comply with HIPAA, VMware offers a Business Associate Agreement (BAA) to all interested customers using our US-based data centers. The BAA was designed in conjunction with a leading law firm with expertise in HIPAA and provides fair and reasonable terms for healthcare providers, insurers, and other organizations. VMware has completed an independent third party examination of vCloud Air against applicable controls of HIPAA.

SOC 1 (SSAE16/ISAE 3402): Service Organization Control (SOC) 1 reports are conducted in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPS). The SOC 1 framework reports on internal controls over financial reporting for any service organization such as VMware vCloud Air. SOC 1 aligns to the International Standard on Assurance Engagements (ISAE) 3402 international reporting standards. SOC 1 examinations are specifically intended to meet the needs of the managements of vCloud Air's customers and vCloud Air's customers' auditors, as they evaluate the effect of the controls at vCloud Air on the clients' financial statement assertions. VMware has completed an independent third-party examination of vCloud Air which spans a twelve (12) month review period.

SOC 2: The Service Organization Control 2 (SOC 2) report is composed of a comprehensive set of criteria on security, availability, processing integrity, confidentiality, and privacy and is similarly set forth by the America Institute of Certified Public Accountants (AICPA). The SOC 2 reports are intended for use by stakeholders (e.g. customers, regulators, business partners, suppliers, directors) of the service organization that have a thorough understanding of the service

organization and its internal controls. VMware has completed an independent third-party examination of vCloud Air that also spans a twelve (12) month review period.

SOC 3: Trust Services Report for Service Organizations Control 3 (SOC 3) reports are designed to meet the needs of customers who want assurance on the controls at a service organization related to security, availability, processing integrity, confidentiality, or privacy. vCloud Air has completed an independent third-party SOC 3 examination of VMware vCloud Air. SOC 3 is composed of a comprehensive set of trust principles including security, availability, processing integrity, confidentiality and privacy.

Cloud Security Alliance: VMware vCloud Air has completed the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ). CAIQ provides industry-accepted ways to document what security controls exist in IaaS, PaaS and SaaS offerings.

FedRAMP Provisional Authority: VMware vCloud Government Service, provided by Carpathian, now has FedRAMP Provisional Authority to Operate issued by the Joint Authorization Board (JAB). FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that can reduce government organizations' costs, time, and staff required to conduct redundant agency security assessments. U.S. government agencies can now leverage vCloud Government Service to meet the stringent security and privacy requirements of FedRAMP.

FIPS 140-2: VMware vCloud Government Service is fully FIPS 140-2 compliant including hardware which provides its 2-Factor Authentication capabilities.

FIPS Pub 199: As discussed previously, vCloud Government Services is certified to store and secure Low Risk Data and Moderate Risk Data as defined by FIPS Pub 199. VMware is willing to work with participating States that require High Risk Data Storage to enhance vCloud Government Services to store and secure this data.

FIPS Pub 199: As discussed previously, vCloud Government Services is certified to store and secure Low Risk Data and Moderate Risk Data as defined by FIPS Pub 199. VMware is willing to work with participating States that require High Risk Data Storage to enhance vCloud Government Services to store and secure this data.

CJIS: vCGS recently underwent a CJIS assessment by CoalFire, Inc. CJIS is not a certification, it is a policy that must be followed and accredited for each deployment which requires it. The goal of VMware's CoalFire assessment was to create a baseline configuration that can be reused across any CJIS opportunity to accelerate the implementation and accreditation timeframes.

FERPA: Like CJIS, FERPA compliance is assessed and confirmed for each deployment that requires it. VMware's vCloud Government Service FedRamp certification and others provide evidence that the underlying infrastructure is capable of meeting rigorous information security and availability requirements. VMware will work with Participating Entities to meet FERPA requirements on a task order basis.

PCI Data Security Standards (DSS): Neither vCloud Air nor vCGS are currently PCI certified at this time. VMware will work with Participating Entities to meet PCI requirements on a task order basis.

IRS Publication 1075: Because both IRS 1075 and FedRAMP are based on NIST 800-53, the compliance boundary for IRS 1075 is the same as the FedRAMP authorization. This, vCGS complies with IRS Publication 1075 on the basis that it is FedRAMP certified.

FISMA: vCGS is FISMA Low and Moderate compliant.

NIST 800-53: NIST 800-53 provides the core controls that must be met to achieve FedRAMP compliance. VMware vCloud Government Service has FedRAMP Provisional Authority to Operate issued by the Joint Authorization Board (JAB), thus we are compliant with NIST 800-53.

NIST SP 800-171: VMware vCloud Government Service has FedRAMP Provisional Authority to Operate issued by the Joint Authorization Board (JAB). NIST 800-171 outlines a subset of the NIST 800-53 requirements, and as stated above, VMware vCloud Government Service is compliant with these guidelines. Since NIST 800-171 outlines a subset of the NIST 800-53 requirements, VMware vCloud Government Service is compliant with NIST SP 800-171.

FIPS 200: Neither vCloud Air nor vCGS are currently FIPS 200 certified at this time. VMware will work with Participating Entities to meet PCI requirements on a task order basis.

VMware AirWatch

The AirWatch Information Security Program is built on the security framework laid out in NIST 800-53.

Although AirWatch is not required to register with any regulatory agencies, we provide a suite of tools for our customer's to maintain industry-relevant compliance guidelines within their mobile device fleets. AirWatch has recently been awarded the HP-IAPP Privacy Innovation Award for Most Innovative Privacy Technology by the International Association of Privacy Professionals (IAPP) for our commitment to delivering an EMM platform focused on end-user privacy. To help ensure the confidentiality, integrity, and availability of our cloud offering, we comply with the European Data Protection Directive (95/46/EC) and our top-tier data center partners have undergone SSAE16 SOC2 Type II audits.

6.6.3 Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center. {8.6.3}

VMware Response:

The VMware Approach to Compliance

Many organizations have initiatives to virtualize their Information Technology (IT) infrastructure, or to move to a Cloud Computing model. However, these initiatives are often complicated by the increasing number of regulatory compliance requirements, which require protection of data such as PCI, HIPAA, FISMA, DIACAP, FedRAMP, GLBA, and other State and Federal requirements. Organizations are increasingly concerned with the complexity, risk, and impact that a new technology can bring to their existing environments.

Historically, most organizations have had to gradually leverage best practices and solutions from a variety of vendors to create a comprehensive IT architecture to meet their unique business and compliance requirements. While each vendor may have their own specific guidance on how to meet compliance, they often do not have guidance on how to meet controls that were not addressed by their specific solutions. This can lead to a delay in the adoption of cloud and virtualization initiatives as it often requires a significant investment in time, resources, and technical capabilities.

VMware addresses these challenges by establishing a Compliance Reference Architecture Framework (RAF), shown in **Figure 13** below, which provides a consistent method for VMware, its partners, and customers to assess and evaluate the impact of regulations on virtual and cloud environments. The intent of the RAF is to provide a single framework for VMware, its partners, and organizations to address a variety of compliance requirements across an IT infrastructure.

The RAF is comprised of four primary components:

- **Use Case**: Provides a business description of an organization and how it has designed its IT architecture to meet specific regulatory and compliance requirements.
- **VMware Product Suites**: VMware's recommended product suites designed to help meet compliance requirements
- **VMware Partner Products**: Provides a framework for partners to address controls that are not covered by VMware's product suites.
- **Organizational Requirements**: Provide guidance on adjacent control requirements not addressed by VMware or Partner solutions such as physical security.

For each Regulation, VMware and its Audit Partners publish three documents in order to elaborate on the subject of sourcing and deploying a vCloud Architecture to operate in a compliant fashion under the prescribed regulation:

Product Applicability Guide (PAG): This document contains an overview of each regulation as it applies to cloud/virtual environments and the mapping of VMware and partner products to specific compliance controls. The PAG addresses the issues of control, applicability and auditability for the specific regulation.

- A description of the VMware product suites (on a product by product basis and relevant changes from previous versions)
- Specific Partner capabilities
- Industry guidance

Architecture Design Guide (ADG): The goal of the Architecture Design Guide is to document design considerations for operating a compliant environment running highly regulated workloads on a VMware vCloud infrastructure.

- Analysis of VMware Technology and partner product capabilities for integration into the VMware Compliance Reference Architecture.
- Business process, enterprise architecture balanced with audit considerations.
- A recommended approach for organizations and their service providers who are required to complete regular compliance assessments.

Validated Reference Architecture (VRA): The goal of this document is to illustrate how the applicable products, coupled with the architecture design and infrastructure component configurations, can be leveraged to provide regulation and governance specific control coverage.

- An analysis of an instance of a vCloud Reference Architecture that is considered to be 'in-situ', e.g. a fully operational point-in-time configuration of both the vCloud Suite or End User Computing software and the regulated application.

- Methods of evaluating controls enabled by the VMware vCloud Suite, EUC products and other third-party graphical or command-line user interfaces through the lens of an auditor.
- Examples that demonstrate alignment with concepts such as "Business-as-Usual" enhanced penetration testing capabilities, etc.

VMware's goal is to deliver a complete solution that helps our customers meet compliance requirements as they look to migrate their business critical applications to cloud computing.

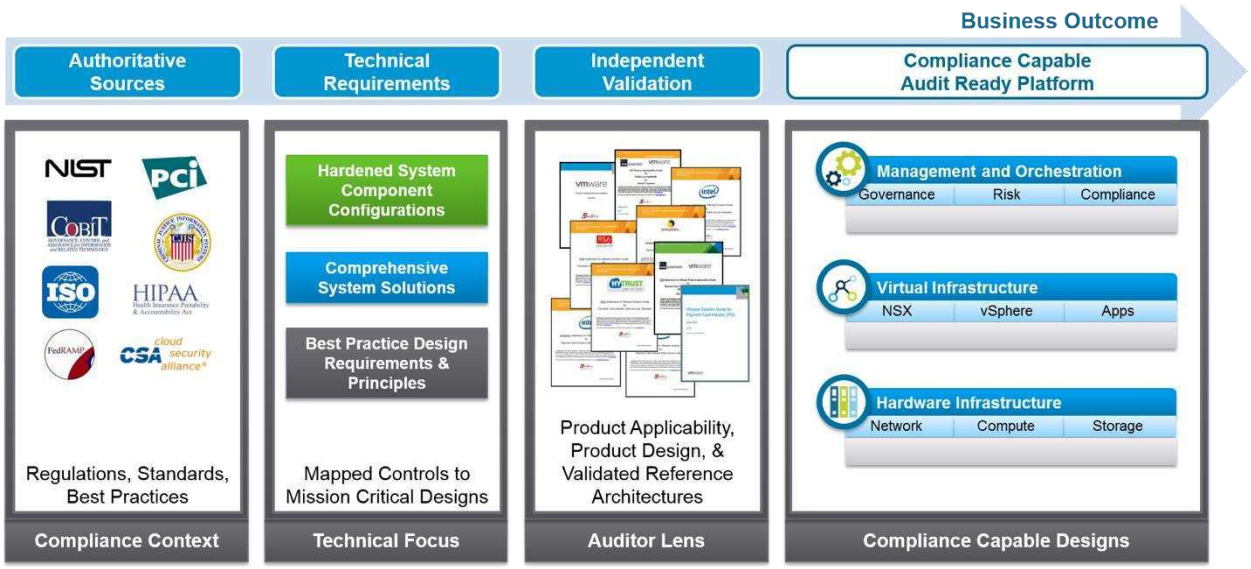


Figure 13. VMware's Compliance Reference Architecture Framework

The vCGS platform includes IDS tools that monitor the IaaS infrastructure and Customers may deploy virtual IDS/IDP within their environment if desired. As described in the vCGS Incident Response Plan (IRP), Carpathia has a policy and process to effectively manage suspected and actual security incidents on the platform. The IRP is consistent with NIST 800-61 Incident Handling Guide and details the process of how Carpathia manages each phase from preparation, containment, analysis, eradication, recovery and retrospective. All Carpathia employees undergo mandatory annual security training, which includes a review of the IRP for employees that are providing system support.

As required per the security baseline, our platform communicates with system stakeholders including the Customer Agency, US-CERT, and the FedRAMP Information System Security Officer (ISSO). The communication flow is dictated based on which stakeholder is the first responder and will also include the customer as a stakeholder in the system support solution.

VMware AirWatch

We designed our security architecture using a defense-in-depth approach to implement multiple layers of security throughout the SaaS environment and to mitigate any potential attacks through multiple safeguards, including:

- Access control mechanisms, firewalls, anti-virus/malware software, auditing mechanisms, network controls, maintaining defined configuration settings, etc.

We perform regular internal scans to assess the vulnerability of our internal network.

6.6.4 Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc). {8.6.4}

VMware Response:

Data Confidentiality Standards and Practices

VMware monitors for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of vCloud Air over which VMware have sole administrative level control. The goal of this process is to identify security incidents and respond to them proactively.

This responsibility stops at any point where customers have control, permission, or access to modify any aspect of the service offering. The customer is responsible for the security of the networks over which they have administrative level control. This includes, but is not limited to, maintaining effective firewall rules, exposing communication ports that are only necessary to conduct business, locking down promiscuous access, and other such capabilities.

Proactive Security Monitoring over Internet and Social Media (e.g. searching filesharing sites for customer data, seeding data with honey tokens) VMware security teams perform OSINT monitoring on the Internet for all VMware products and services. This includes harvesting data from search engines, le sharing, and social networking sites. This data is analyzed for keywords and other specific indicators.

With regards to potential data leaks, the customer is solely responsible for protecting the security of his or her content, including any access provided to employees, customers or third parties.

vCloud Air provides certain software and functionality to help protect content from unauthorized access such as firewalls, load balancers, and IPsec VPNs. Customers are encouraged to deploy additional security mechanisms similar to what exists in their current data center to address other security controls such as data encryption, intrusion detection, le integrity monitoring, and other such concerns relevant to the sector and regulatory requirements that apply to the specific business of a customer.

Security Organization and Operations

VMware maintains multiple security teams responsible for different aspects of delivering both products and services, as well as protecting VMware corporate networks.

- VMware has a dedicated Security Product Line Manager responsible for ensuring adequate security controls and features within the VMware Service offering.
- VMware has a product security team responsible for evaluating VMware software and products for vulnerabilities. They work closely with R&D and engineering teams to ensure secure coding practices and publish security related advisories.
- VMware has an Information Security team responsible for securing VMware cloud services, setting security standards and policy, and the deployment and implementation of new security technologies.

- VMware has a dedicated 24/7/365 Security Operations team that is responsible for monitoring VMware cloud services. They perform incident response, forensic investigations, and OSINT monitoring. They also ensure adherence to internal policies and standards.
- VMware security teams hold multiple certifications from ISC2, GIAC, as well as others relevant for their particular areas of expertise and focus. Several VMware security team members also hold security clearances with the Department of Defense, and are members of other organizations such as the FBI Infragard program and the HTCIA.
- All VMware employees participate in continuing education, training, and certification.
- VMware performs background checks on all new hires. This includes verifying SSN, deemed export control/DPL, education, employment, as well as criminal history.

Prevention of Exposure to Unauthorized Personnel

VMware does not have access to customer data, operating systems, or access into a customers configured networks. VMware's access control, separation of duty, and other policies define which individuals are allowed to have access to vCloud Air management systems.

Managing and Reviewing Administrators Access to Stored Data

Although VMware does not have access to customer data, operating systems, or customer networks, they do have administrative access to vCloud Air management systems. This access is reviewed on a quarterly basis according to our internal policies and procedures as well as industry best practices. In addition, if an employment is terminated for any reason, user credentials are immediately revoked to prevent access to vCloud Air and all other VMware systems.

VMware AirWatch

AirWatch classifies all customer data as confidential and secures it accordingly. Access controls are technically enforced and permissions are provisioned according to role and business need. All access to the SaaS environment is logged and monitored: Customers can use the built-in reporting capabilities in the console to monitor access to the AirWatch solution.

AirWatch-issued computers are secured with strong password requirements.

6.6.5 Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp), and certifications relating to data security, integrity, and other controls. {8.6.5}

VMware Response:

VMware IaaS Services

The International Organization for Standardization (ISO) has developed he ISO 27001 standard which defines an information security management system (“ISMS”) as a systematic approach to managing sensitive company information so that it remains secure. It includes an organization’s people, processes and IT systems and the application of a risk management process.

vCloud Air has established and implemented an ISMS based on ISO 27001 standards to manage risks relating to confidentiality, integrity, and availability of information.

vCloud Air engages an independent third party auditing firm on an on-going basis to validate vCloud's air adherence to the ISO 27001 standard. VMware's ISO 27001 certificate number 1670797-9 was originally registered on June 28th, 2013 and was issued on December 2nd, 2015. This certificate was issued by 3rd party auditor Schellman (formerly Brightline) to record their validation of VMware vCloud Air's adherence to the standard. The scope of the ISO/IEC 27001:2013 certification is limited to the information security management system (ISMS) supporting the management of the infrastructure and services used to support the VMware vCloud Air and in accordance with the statement of applicability version 2.0. Assets within the scope of the ISMS include: information, software, databases, hardware, and VMware vCloud Air employees supporting the vCloud Air service offering.

VMware AirWatch

The AirWatch Information Security Program is built on the security framework laid out in NIST 800-53 rev. 4.

Although AirWatch is not required to register with any regulatory agencies, we provide a suite of tools for our customer's to maintain industry-relevant compliance guidelines within their mobile device fleets. AirWatch has recently been awarded the HP-IAPP Privacy Innovation Award for Most Innovative Privacy Technology by the International Association of Privacy Professionals (IAPP) for our commitment to delivering an EMM platform focused on end-user privacy. To help ensure the confidentiality, integrity, and availability of our cloud offering, we comply with the European Data Protection Directive (95/46/EC) and our top-tier data center partners have undergone SSAE16 SOC2 Type II audits and have ISO 27001 certifications.

6.6.6 Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.{8.6.6}

VMware Response:

VMware IaaS Services

In accordance with our ISO and SOC commitments, change-related activity, including administrative actions, performed on the management infrastructure layers supporting vCloud Air and vCGS are monitored and logged to a centralized logging server for a minimum of 1 year. Infrastructure logging is in place for customer interactions with the vCloud Air and vCGS management and administrative consoles. These logs are only for the management and administrative interfaces.

These are not in place for monitoring of individual customer VMs installed within the customer tenant org. Limited logging and activity reporting are available from customer tenant environments, with more detailed reporting, auditing and logging capabilities introduced Q4-2014.

VMware AirWatch

We have full auditing capabilities on all environments in the AirWatch Cloud to enable user accountability. Customers can use the built-in event log, customizable dashboards, integrated reporting engine and AirWatch Hub to audit the web console and end-user actions.

For the SaaS environment logs, our Information Security Team helps ensure that systems generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Maintaining Security Compliance

VMware maintains security certifications for its cloud services through continuous monitoring, periodic internal and external audits, application of all patches on a regular basis, through proactive penetration testing, and by adhering to our audited policies and procedures. VMware complies with all required re-certifications and audits to ensure that we remain certified and compliant.

6.6.7 Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups. {8.6.7}

VMware Response:

VMware IaaS Services

The vCloud Air and vCGS Terms of Service and Data Privacy Addendum's establish the line of demarcation between the responsibility of VMware and the customer as it pertains to data protection. In addition, security whitepapers are made available to customers to further illustrate these points or to establish transparency regarding the separation of responsibility between VMware and the customer for compliance programs such as HIPAA or PCI.

Subscribers are able to use a VPN connection at multiple layers to maintain data security. For traffic in motion, VPNs can be created for a particular application and also for an entire virtual data center. A site-to-site IPsec-VPN can also be established to securely tunnel the entire virtual data center back to the private data center. For data "at rest", subscribers are provided a role-based access control, whereby specified users are not exposed to the entire infrastructure and can be limited to a single or multiple virtual data centers.

Further details of the controls in place to limit exposure of these groups to customer data is documented within the ATA 101 and SOC reports, available under NDA.

vCloud Air and vCGS have logically separated networks that restrict Tenant access to only their own private networks. VMware vCloud Air and vCGS has two offerings: The Dedicated Cloud option provides physically isolated and reserved compute resources from all other vCloud Air and vCGS tenants, as well as a private cloud instance. The Virtual Private Cloud option has a multitenant compute resource mode. Both services have logically isolated networking and storage that ensures secure resource separation. Customers have complete control over the file systems and databases they deploy within the service.

VMware AirWatch

Access is technologically enforced and employees are only authorized the level of access to information assets that is required to meet an approved business need or perform prescribed job responsibilities. Administrative access is limited to only those users that explicitly require privileged access.

Customers do not have direct access to the SaaS environment; rather, customers administer the solution via the Web console.

AirWatch has the ability to restrict visibility of customer hosted data or documents to specific users or groups. This can be done between tenants and within a single tenant. The platform supports hierarchical multi-tenancy, meaning that tenants are logically separated using firewalls and encryption to prevent access of one tenant's data or applications by any other tenant. In addition tenants can institute their own multi-tenancy for different lines of business within their own AirWatch cloud.

6.6.8 Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored. {8.6.8}

VMware Response:

VMware IaaS Services

If VMware determines that there has been unauthorized access to, or use or disclosure of, Your Content, or other incident VMware will use commercially reasonable efforts to notify You, taking into account any applicable law, regulation, or governmental request.

VMware will provide security incident response (e.g., detection, severity/threat classification, forensics, and resolution) pertaining to management infrastructure over which VMware has direct, administrative, and/or physical access and control, such as the vCloud Air and vCGS servers, storage, applications, and network devices.

Documented escalation procedures and a ticketing system are in place to guide employees in identifying, reporting, and responding to system availability issues and related security incidents. This includes an incident response policy to determine severity of an incident and a breach notification process.

All alerting and monitoring at the guest OS\VM level is the responsibility of the customer.

In the event of a data breach customers will be notified by VMware vCloud Air Global Support Services via their preferred contact means. VMware will provide security incident response (e.g., detection, severity/threat classification, forensics, and resolution) pertaining to management infrastructure over which VMware has direct, administrative, and/or physical access and control, such as the vCloud Air service servers, storage, applications, and network devices.

Notification timeframes are agreed upon between VMware and the customer in standard agreements and contracts. Incidents are handled on a case-by-case basis, but typically occur between 24-48 hours after a breach has been confirmed.

VMware will provide security incident response (e.g., detection, severity/threat classification, forensics, and resolution) pertaining to management infrastructure over which VMware has direct, administrative, and/or physical access and control, such as the vCloud Air service servers, storage, applications, and network devices.

6.6.9 Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers. {8.6.9}

VMware Response:

VMware IaaS Services

At the tenant level, firewall services are provided via the vCloud Networking & Security Edge Gateways or optionally by NSX for customers to configure and maintain. Firewall policies can be used to restrict and manage public/Internet-based traffic and create DMZ zones for multi-tier applications. Firewall policies can also be used to configure access policies between internal IP networks and VxLAN segments. Stateful inspection firewalling can be applied on the external interface of the vCNS Edge Gateway.

VMware architects, provisions, monitors and manages the vCloud Air infrastructure and surrounding components. As described in the AT 101 (ISO 27001) report, access points such as delivery and loading areas and other points where unauthorized persons may enter the premises are controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. The details of this control are not disclosed publicly.

VMware AirWatch

We implement multiple security measures to protect hosted servers, including physical and logical controls.

6.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS) {8.6.10}

VMware Response:

VMware IaaS Services

vCloud Government Service has a current FedRAMP Joint Approval Board (JAB) Provisional Authority to Operate (PATO), which certifies that we comply with NIST controls for an Infrastructure as a Service Cloud offering. The System Security Plan is on file with the FedRAMP PMO. This plan outlines the requested information in greater detail and can be accessed via request to the FedRAMP PMO at FedRAMP PMO, General Services Administration 1800 F Street, Washington, DC 20006 or by email at info@fedramp.gov.

VMware AirWatch

AirWatch can provide sample architecture diagrams under NDA to Participating Entities during task order negotiations as required.

6.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data. {8.6.11}

VMware Response:

All employees that are hired by VMware must first go through a background investigation process. Specific to our cloud services, information security policies and procedures have been implemented regarding the protection of information assets. The policies and procedures act as a guide for all vCloud Air personnel. These policies and procedures define guidelines for the vCloud Air security program, which includes implementing and managing logical access security and controls, including the following:

- Information security policy
- Data classification and handling policy
- Acceptable use policy
- Password policy

These policies are reviewed and approved by management on at least an annual basis.

6.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit. {8.6.12}

VMware Response:

Data at rest encryption is the responsibility of the customer. As an example, HyTrust is an endpoint encryption choice for many vCloud Air customers.

Data in transit will be encrypted based upon the customers selected method of transport (SSL or IPSEC VPN). IPSec protocols include ESP tunnel mode for data/payload security and IKE-v1 for a two-phase authentication. The service supports both the pre-shared key and the certified authentication mode and leverages 128-byte and 256-byte AES encryptions for data in transit.

6.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach. {8.6.13}

VMware Response:

If VMware determines that there has been unauthorized access to, use of, or disclosure of customer content, VMware will use commercially reasonable efforts to notify customers taking into account any applicable law, regulation, or governmental request. Please refer to Section 6.3.1 of our response for a detailed write up on notification process to the State and Cardholders in the event of a data breach.

6.7 MIGRATION AND REDEPLOYMENT PLAN {8.7} (E)

6.7.1 Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely de-provisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration. {8.7.1}

VMware Response:

VMware IaaS Services

Upon termination of vCloud Air and/or vCGS service, VMware will take a final snapshot of the purchasing entity's primary database storage and retain it for 90 days, after which VMware may purge the final snapshot. VMware may immediately purge all other data associated with the database instances upon termination (including snapshot, PITR backup) except for the final snapshot.

VMware AirWatch

At the end of the contract, AirWatch will assist the customer in using solution controls to export data. Customers in a Dedicated Cloud deployment can leverage a robust data mart. Data is secured in transmission.

We maintain standard SLAs with our customers to provide for unscheduled downtime.

- SLAs are defined within the VMware AirWatch Policy.

Per our Hosted Services Policy, we provide outage credits in the event of a service interruption:

- "AirWatch warrants it will provide Availability of the Hosted Services 99.9% of the calendar month (the "Service Level"). To the extent that the Hosted Services fail to conform to the Service Level, Customer may request service credits ("Outage Credits") as provided herein. A failure or lack of Availability for any period of time of at least one minute during which Customer is unable to utilize the Hosted Services due to AirWatch's failure to provide Customer with the specified services constitutes an "Outage". All Outage measurements will be rounded up or down to the nearest one-minute increment, with increments equal to or greater than 30 seconds being rounded up to the next minute. Outage Credits are based on cumulative periods of Outage over a calendar month. Final determinations of the length of the cumulative periods of Outage over a calendar month shall be based on AirWatch's internal monitoring equipment and records. Outage Credits will be taken against only the Hosted Service fees for the month in which the Outage occurred."

6.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer. {8.7.2}

VMware Response:

VMware IaaS Services

One of the key advantages of using vCloud Air and vCGS is the ease with which customers can move data into and out of the environment. Customers can, at any time, use VMware's proven vMotion capability to move their workloads and data from vCloud Air or vCGS to their on-premises environment.

VMware AirWatch

At the end of the contract, AirWatch can assist the customer in using solution controls to export data. Customers in a Dedicated Cloud deployment can leverage a robust data mart. Data is secured in transmission.

- AirWatch has defined data retention and data disposal policies to safeguard data throughout its lifecycle.

Please refer to the answer provided above and to Clause 10 of the VMware End User License Agreement which is included as **Appendix C** of this proposal, and as updated, as required, online for additional information regarding end of contract terms.

6.8 SERVICE OR DATA RECOVERY {8.8} (E)

6.8.1 Describe how you would respond to the following situations; include any contingency plan or policy. {8.8.1}

a. Extended Downtime {8.8.1.a}

VMware Response:

VMware IaaS Services

VMware vCloud Air leverages proven VMware High Availability technology to minimize the risk of extended downtime. Although the availability of customer workloads is highly dependent on their architecture, VMware provides the capabilities required to minimize the possibility of extended downtime. For example, VMware offers several geographically distributed data centers, along with VMware Dynamic Resource Scheduler, VMware High Availability, VMware local and long distance vMotion, VMware Data Protection, and VMware Advanced Networking capabilities such as VMware NSX software defined networking. VMware also offers training and support along with professional services and pre-sales engineering to assist Participating Entities in minimizing downtime.

That said, in the unlikely event that an extended outage does occur, VMware will support the customer's efforts to restore services to an alternate vCloud Air or vCGS datacenter. We will also provide remedies in the form of service credits as outlined in the following VMware vCloud Air, vCGS, VMware AirWatch, and VMware Identity Manager SLAs. For details on service credits please see each service's SLA. These are provided in **Appendix C**.

b. Suffers an unrecoverable loss of data {8.8.1.b}

VMware Response:

VMware IaaS Services

As defined in our Terms of Service, the customer is ultimately responsible for any losses or other consequences arising from the failure to encrypt or back up their content.

However, as discussed in detail in section 6.8.2.a below, VMware IaaS services are architected to minimize the risk of unrecoverable data loss. In addition option services such as vCloud Air Data Protection can be leveraged to further mitigate any risk. VMware's vCloud Air policy regarding data loss can be found in the vCloud Air Terms of use in **Appendix C**. VMware's vCloud Government Service policy regarding data loss can be found in the vCloud Government Service Terms of Service in **Appendix C.**

VMware AirWatch

AirWatch Business Continuity and Disaster Recovery strategies include data and hardware redundancy, network configuration redundancy and backups, and robust, regular testing exercises. AirWatch features active-passive configurations for high availability and redundancy with all components made to failover with minimal downtime. Load balancing capabilities are deployed across multiple data centers to ensure timely server recovery. AirWatch also incorporates replication technology featuring SQL log shipping or network SAN byte replication to prevent data loss.

c. Offerors experiences a system failure {8.8.1.c}

VMware Response:

VMware IaaS Services

In the case of short term system failures and outages, VMware's service level agreement outlines remedies including service credits. If a particular class of service is Unavailable for 24 consecutive hours, then you may request a Chronic SLA Credit. A "Chronic SLA Credit" is an amount equal to 100% of the monthly Service Offering recurring or metered (as applicable)

subscription charges invoiced by VMware, for the affected class of service, in the calendar month in which the SLA Credit is due. Any Chronic SLA Credit is in lieu of any SLA Credits that might be otherwise due.

VMware has provided guidance regarding service failure in the Service Level Agreement, Terms of Service, and Data Privacy Addendum these documents are provided in **Appendix C**.

VMware AirWatch

VMware vCloud Air and VMware AirWatch Business Continuity (BC) strategies include clear policies and procedures as well as robust, regular testing exercises. Our BC recovery strategies for support and maintenance include provisions for workforce mobility, secondary support locations, and defined leadership roles and responsibilities for all recovery staff.

- Multiple Support Locations – AirWatch maintains a Global Support Team, which spans multiple offices around the world. This ensures that if a disaster occurs at one of our offices, our remaining Support Team members can provide assistance to our customers.
- Mobile Workforce – Should an AirWatch office become inaccessible, all AirWatch employees are equipped with laptops and can access necessary internal resources.
- Defined Leadership – During a disaster, roles and responsibilities are assigned to key personnel, and a recovery manager provides leadership and documents the continuity process. Additionally, emergency contact numbers for key personnel are provided for all vendors and support staff.

d. Ability to recover and restore data within 4 business hours in the event of a severe system outage. {8.8.1.d}

VMware Response:

VMware IaaS Services

VMware vCloud Air and vCGS provide the ability to recover and restore data well within 4 business hours in the event of a severe system outage. VMware vCloud Air has defined SLAs to provide between 99.95% and 99.99% availability measured monthly for each of its services. This equates to maximum downtime of between or 4 minutes 23 seconds and 21 minutes 54.9 seconds of total cumulative downtime per month. VMware vCloud Government Service has defined SLAs to provide between 99.9% and 99.95% availability measured monthly for each of its services. This equates to maximum downtime of between 21 minutes 54.9 seconds and 43 minutes 49.7 seconds of total cumulative downtime per month. See **Appendix C** for SLA details for each service.

We have a fully staffed operations team 24/7/365 to address any system outages as quickly as possible and aim to minimize the downtime of any given event to well below four hours.

Documented escalation procedures and a ticketing system are in place to guide employees in identifying, reporting, and responding to system availability issues and related security incidents. This includes an incident response policy to determine severity of an incident and a breach notification process.

We can discuss specific recovery information under NDA to Participating Entities during task order negotiations as required.

VMware AirWatch

We can discuss specific recovery information under NDA to Participating Entities during task order negotiations as required.

e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO). {8.8.1.e}

VMware Response:

There is no stated RPO or RTO for the service outside of the SLA targets provided and discussed in the section 6.8.1.d above. VMware, Inc. has developed Business Continuity and Disaster Recovery Programs for responding to events that significantly disrupt the company's business operations. Because the timing and impact of disasters and disruptions is unpredictable, VMware's Programs allow for flexible responses to actual events as they occur.

VMware AirWatch

AirWatch Business Continuity (BC) and Disaster Recovery (DR) strategies include data and hardware redundancy, network configuration redundancy and backups, and robust, regular testing exercises.

- Business Continuity – Our BC recovery strategies for support and maintenance include provisions for workforce mobility, secondary support locations, and defined leadership roles and responsibilities for all recovery staff.
- Multiple Support Locations – AirWatch maintains a Global Support Team, which spans multiple offices around the world. This ensures that if a disaster occurs at one of our offices, our remaining Support Team members can provide assistance to our customers.
- Mobile Workforce – Should an AirWatch office become inaccessible, all AirWatch employees are equipped with laptops and can access necessary internal resources.
- Defined Leadership – During a disaster, roles and responsibilities are assigned to key personnel, and a recovery manager provides leadership and documents the continuity process. Additionally, emergency contact numbers for key personnel are provided for all vendors and support staff.
- High Availability and Disaster Recovery – AirWatch features active-passive configurations for high availability and redundancy with all components made to failover with minimal downtime. Load balancing capabilities are deployed across multiple data centers to ensure immediate server pick up, ensuring zero end user downtime. AirWatch also incorporates replication technology featuring SQL log shipping or network SAN byte replication to prevent data loss.

6.8.2 Describe your methodologies for the following backup and restore services: {8.8.2}

a. Method of data backups

VMware Response:

VMware IaaS Services VMware vCloud Air Backup and Restore Services

VMware will provide the following services to Participating Entities with respect to Data Recovery:

- Data protection, such as routine backups, for the vCloud Air and vCGS infrastructure, including top-layer management and user-management interfaces owned and operated by VMware.
- Data and infrastructure restoration for the vCloud Air and vCGS infrastructure, including top-layer management and user-management interfaces owned and operated by VMware.

Participating Entities will be responsible for the following services with respect to Data Recovery for a fee:

- Data protection, such as routine backups, for the data and content accessed or stored on vCloud Air and vCGS virtual machine's or storage devices, configuration settings, etc.
- Data, content, virtual machine and configuration restorations for assets accessed or stored on your vCloud Air and vCGS account.

Data Protection is an optional service that provides secure, image-based backup and recovery capabilities that enable you to protect important virtual machine data and content hosted in your vCloud Air IaaS environment. Through the Data Protection administration interface available in the vCloud Air Console, vApps and their virtual machine members can be selected for policy-based backup and recovery operations.

Data Protection feature subscription and activation may be requested via My VMware and is subject to additional service fees based on the amount of backup data capacity. Backup data capacity for the service is measured in front end terabytes (FETB). Once activated, vApps and their virtual machine members may be registered and unregistered with Data Protection features on a self-service basis through the vCloud Air Console.

As part of this service, VMware will:

- Implement and maintain central service components (backup software appliances, backup and archival storage media and associated network topologies) needed to support Data Protection features.
- Perform routine configuration, maintenance and optimization services on behalf of the Data Protection environment and in conformance with industry best practices.
- Allocate requisite backup storage based on capacity selections made at the time of subscription enrollment.
- Guarantee storage locality per geographical region for all backup data.
- Provide necessary Data Protection service reporting as it is requested.

Participating Entities will be responsible for:

- Subscribing to Data Protection as an add-on feature via My VMware and selecting an amount of backup storage capacity commensurate with your requirements.
- Creating custom backup protection policies that may include, but are not limited to: affinity settings per VDC, scheduling, and retention periods.
- Registering and unregistering individual vApps and their virtual machine members for scheduled backups using Data Protection.
- Performing any on-demand backups per vApp and its virtual machine members.
- Performing in-place or out-of-place restores per vApp and/or individual virtual machine.
- Managing any in-guest recovery tasks, including restore operations at the operating system, file systems and/or any application level.

- Managing backup storage capacity and consumption that may include, but is not limited to: activity reporting, ordering additional storage capacity via My VMware and deleting any backup data in inventory to free up space.

For additional information see coverage of VMware Data Protection in section 8.1.1.3 of this document.

VMware AirWatch Services

VMware AirWatch maintains server images for hosted customers to help enable secure imaging procedures.

b. Method of server image backups

Server Images backups are handled in the same manner as described for data backups in section 8.8.2.1.a above.

c. Digital location of backup storage (secondary storage, tape, etc.)

When discussing backup of VMware vCloud Air services, there are two levels of backup to touch upon – the backup of the underlying infrastructure that delivers vCloud Air and the backup of customer workloads.

Backup of VMware vCloud Air Infrastructure

VMware is responsible for the underlying infrastructure. vCloud Air has failover capability for the primary production data centers to backup production data centers in the event the primary data center experiences significant loss. This is done by using VMware's proven Site Recovery Manager for applications, EMC replication and backup technology for SAN and NAS storage, and multiple industry leading technologies for redundant networking. Application data and data bases in primary production data centers are also locally backed up as per documented VMware policies and these backups are also sent to the backup production data centers using EMC's Networker and Avamar products.

Backup of Customer Workloads

Backup of the customer workload is the responsibility of the customer. We offer a Data Protection Service which is a self-service backup to the same data center site, but in a different storage solution. Customers can purchase Rackware to provide geographical HA and COOP, but this service is not provided as a core capability of vCloud Air or vCGS. Finally, customers may also leverage their preferred 3rd party agent-based backup tools to backup to offsite locations. For additional details, see the answer to 6.8.2.a above.

d. Alternate data center strategies for primary data centers within the continental United States.

Customers who wish to back-up their workloads to an alternative data may do so. VMware vCloud Air and vCGS services are offered from multiple datacenters within the United States and around the world. Each datacenter serves as an alternate for one other data center. **Figure 14**

below identifies the locations of these datacenters. Participating Entities have the ability to identify their primary and alternate data center locations at the time of deployment.

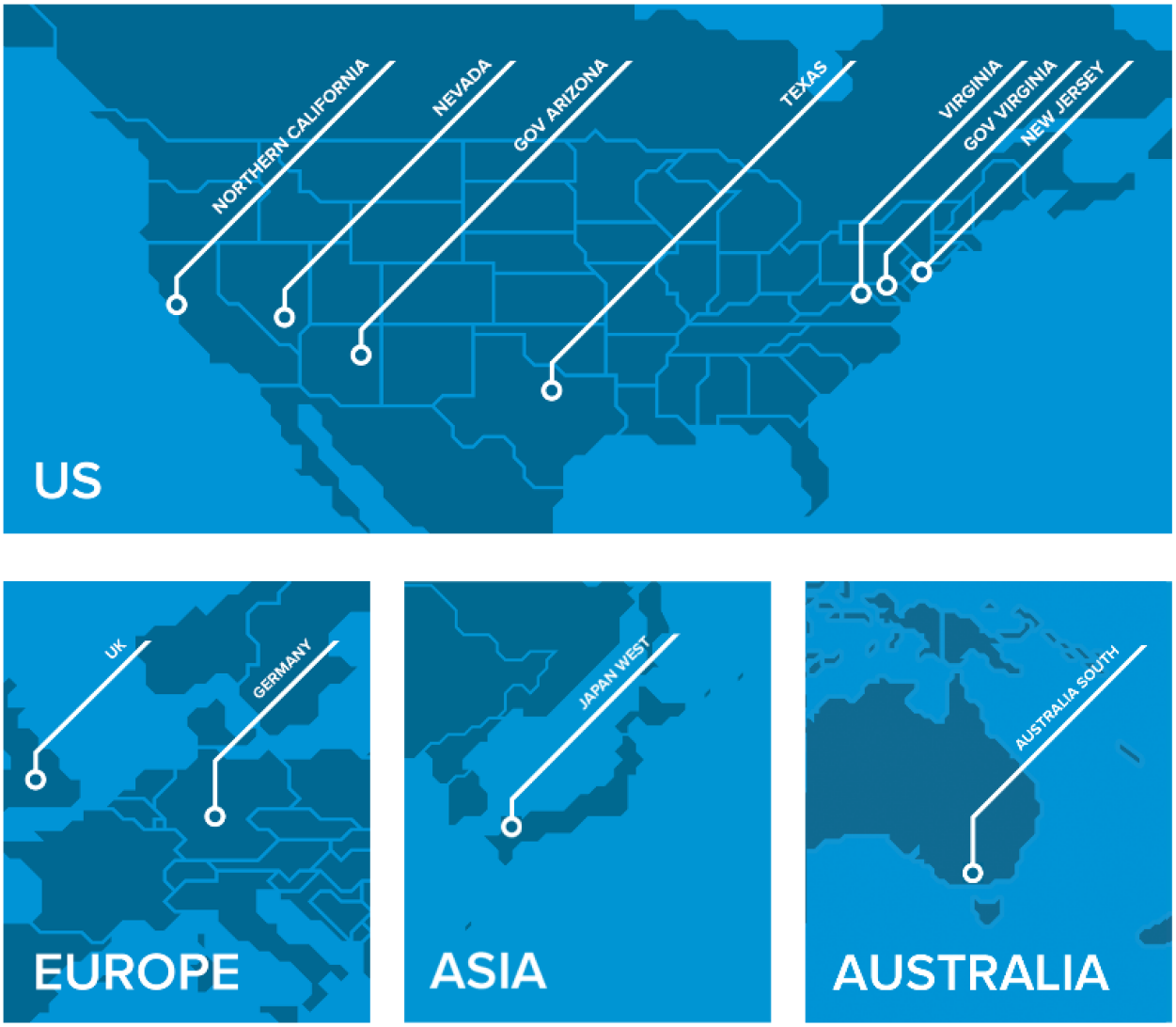


Figure 14. VMware vCloud Air and vCloud Government Service Data Center Locations

VMware AirWatch

AirWatch backs up the production environment from the primary US data center to the secondary US data center.

6.9 DATA PROTECTION {8.9}(E)

6.9.1 Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest. {8.9.1}

VMware Response:

VMware IaaS Services

Data in transit will be encrypted based upon the customers selected method of transport (SSL or IPSEC VPN). IPSec protocols include ESP tunnel mode for data/payload security and IKE-v1 for a two-phase authentication. The service supports both the pre-shared key and the certified authentication mode and leverages 128-byte and 256-byte AES encryptions for data in transit.

Data at rest encryption is the responsibility of the customer. By example HyTrust is an endpoint encryption technology that is used by vCloud Air customers.

VMware AirWatch

AirWatch leverages strong, non-proprietary encryption algorithms to protect applicable data at rest and in transit.

6.9.2 Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity. {8.9.2}

VMware Response:

VMware IaaS Services

VMware is willing to sign relevant and applicable Business Associate Agreements or other agreements that may be necessary to protect data with a Purchasing Entity. Final signature will depend upon the scope of the agreement which will be negotiated with the Purchasing Entity as part of task order negotiations.

To help customers comply with HIPAA, VMware offers a Business Associate Agreement (BAA) to all interested customers using our US-based data centers. The BAA was designed in conjunction with a leading law firm with expertise in HIPAA and provides fair and reasonable terms for healthcare providers, insurers, and other organizations. VMware has completed an independent third party examination of vCloud Air against applicable controls of HIPAA.

VMware AirWatch

Business Associate Agreements are not applicable to VMware AirWatch. AirWatch does not meet the definition of a Business Associate under HIPAA, nor do we receive PHI. However, we provide tools in our product to help our Healthcare customers remain HIPAA-compliant.

6.9.3 Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP. {8.9.3}

VMware Response:

VMware IaaS Services

VMware does not access customer data in any way. Our role based access controls and security technology prevent access to customer data by VMware and subcontractor staff. VMware will not use customer account or usage data for any purposes other than those defined in the Master Agreement, participating addendum, or related service level agreement. VMware cannot access Government data and therefore cannot perform data mining on it. VMware nor its resellers will not perform data-mining on government related data or use government related data for any other purpose.

Neither VMware nor its resellers will resell or otherwise redistribute information gained from its access to the data received as a result of this RFP with the exception of data required to allow the customer to license third party software such as operating systems as defined in the Third Party Terms found in **Appendix C**, VMware will prohibit its resellers and employees from reselling, redistributing, or using data in any way other than those defined in the Master Agreement, participating addendum, or related service level agreement using policies and procedures and subcontract agreements.

VMware AirWatch

Information contained in this response is to be used for evaluator purposes. We do not use customer solution data for testing, development, data mining purposes, etc.

Please refer to the AirWatch End User License agreement in **Appendix C** for additional information regarding data collection and use.

6.10 SERVICE LEVEL AGREEMENTS {8.10} (E)

6.10.1 Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement. {8.10.1}

VMware Response:

VMware has included its current Service Level Agreements (SLA) in Appendix C. VMware's SLAs are specific to each product and service, and are subject to the product's Terms of Service (which are also provided). The SLA is specific to the product rather than to the customer, to define the expected availability and recourse should the product not meet the stated availability levels. VMware's existing customers include Federal, State and Local government customers as well as commercial customers, who successfully utilize our products in accordance with the current SLA and Terms of Service and their applicable, mandatory laws and regulations. Accordingly, VMware is confident that the existing SLA meets the state and local government requirements, as it is being utilized currently.

VMware IaaS Services

To best work with our customers and improve our terms in alignment with market requirements, VMware is willing to review the terms of its SLA during negotiations of the Participating Addendum to identify how the existing SLA meets the state's applicable and mandatory laws and regulations. If it becomes apparent to the parties that it is necessary to revise VMware's SLA to comply with the state's applicable and mandatory laws, VMware will enter into discussions about how to best address these requirements

VMware SaaS Services

VMware AirWatch Service Level Agreements are non-negotiable. As a multi-tenant platform, all users of VMware AirWatch can expect a comprehensive SLA, which offers a guaranteed uptime SLA of 99.9%.

Keeping a standardized set of SLAs allows for a standard set of capabilities, processes and procedures which in turn reduces risk of failures and outages due to human error or non-standard system configurations. AirWatch strives to continuously improve its products and services as well as its SLAs. Our goal is to provide SLAs which are on par or better than industry standard and that meet the needs of all customers.

6.10.2 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements. {8.10.2}

VMware Response:

Please refer to **Appendix C** of our response for the full description of VMware's SLAs. Our SLAs define our performance, events, and remedies.

6.11 DATA DISPOSAL {8.11} (E)

Specify your data disposal procedures and policies and destruction confirmation process {8.11}

VMware Response:

VMware IaaS Services

As described previously in section 6.7, upon termination, VMware will take a final snapshot of the participating entity's primary database storage and retain it for 90 days, after which VMware may purge the final snapshot. VMware may immediately purge all other data associated with the database instances upon termination (including snapshot, PITR backup) except for the final snapshot.

VMware does not explicitly destroy customer data beyond re-formatting of storage volumes upon customer termination. In addition, VMware does not perform hardware-level data destruction (degaussing, hard drive destruction, etc.) at present.

Encrypted in-guest volumes are recommended for customers with requirements for more advanced data isolation and security.

VMware AirWatch

AirWatch has defined data retention and disposal procedures to help ensure data security throughout the full lifecycle.

6.12 PERFORMANCE MEASURES AND REPORTING {8.12} (E)

6.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability. {8.12.1}

VMware Response:

Please refer to **Appendix C** of our response for the full description of VMware's SLAs. Provided below are the specific sections to address each question.

IaaS – vCloud Air

Provided in **Table 34** below are VMware's SLAs for vCloud Air. Our Availability Commitment ranges from 99.99% - 99.95 based on the Class of Service. The SLAs are subject to the terms of the applicable Terms of Service for the VMware vCloud Air Service Offerings.

Class of Service	Availability Commitment
Dedicated Cloud	99.99%
Virtual Private Cloud	99.95%
Data Protection	99.95%
Disaster Recovery	99.95%
Virtual Private Cloud OnDemand	99.95%

Table 34. vCloud Air SLAs

IaaS – Object Storage

Provided in **Table 35** below are VMware's SLAs for Object Storage. Our Availability Commitment ranges from 99.9% - 99.0% based on the Class of Service. The SLAs are subject to the terms of the applicable Terms of Service for the VMware vCloud Air Service Offerings.

Class of Service	Availability Commitment
Object Storage powered by Google Cloud Platform (Standard)	99.9%
Object Storage powered by Google Cloud Platform (Durable Reduced Availability)	99.0%
Object Storage powered by Google Cloud Platform (Nearline Storage)	99.0%

Table 35. vCloud Air Object Storage SLAs

IaaS – vCloud Government Service

Provided in **Table 36** below are VMware's SLAs for vCloud Government Service. Our Availability Commitment ranges from 99.95% - 99.9% based on the Class of Service. The SLAs are subject to the terms of the applicable Terms of Service for the VMware vCloud Government Service Offerings.

Class of Service	Availability Commitment
Dedicated Cloud	99.95%
Virtual Private Cloud	99.9%

Table 36. vCloud Government Service SLAs

VMware will use commercially reasonable efforts to ensure that each class of service purchased for an identified user of an instance of a Service Offering ("you" or "Customer") is "Available" during a given calendar month equal to the "Availability Commitment" provided in **the Tables 35 and 36** above.

SaaS – VMware AirWatch

Our Availability Commitment for VMware AirWatch is 99.9%. The SLAs are subject to the terms of the applicable Terms of Service for VMware AirWatch.

SaaS – VMware vRealize

VMware will use commercially reasonable efforts to ensure that each unique vRealize Air service instance purchased by a customer of the Service Offering ("you" or "Customer") is "Available" during a given calendar month equal to 99.9% ("Availability Commitment").

6.12.2 Provide your standard uptime service and related Service Level Agreement (SLA) criteria. {8.12.2}

VMware Response:

VMware's standard uptime and SLA criteria is provided in **Appendix C** of our response.

6.12.3 Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability. {8.12.3}

VMware Response:

If a customer needs to open a case for product technical support, they may do so by calling our VMware Support Department at 1-877-486-9273. Additionally, the customer may contact the VMware NASPO Contract Manager (CM) as provided in section 5.1 of our response. The CM can assist the customer with opening the support case.

Once the case has been opened with the VMware support team, VMware technical staff will assist the customer to resolve the issue. The VMware support team is available 24 hours a day / 7 days a week.

6.12.4 Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time. {8.12.4}

VMware Response:

IaaS – vCloud Air and vCloud Government Service

If the Availability of a class of service that you purchase is less than the associated Availability Commitment, then you may request Service Credits for that affected class of service. Availability in a given month is calculated according to the following formula:

"Availability" = ((total minutes in a calendar month – total minutes Unavailable) / total minutes in a calendar month) x 100

A class of service will be considered "Unavailable," subject to the Service Level Agreement Limitations set forth below, if VMware's monitoring tools determine one of the following events

has occurred ("SLA Event"). The total minutes that a class of service is Unavailable for a particular SLA Event is measured from the time that VMware validates the SLA Event has occurred, as defined below, until the time that VMware resolves the SLA Event such that the Service Offering is Available to you. If two or more SLA Event occurs simultaneously, the SLA Event with the longest duration will be used to determine the total minutes Unavailable.

1. Each of the following will be considered an SLA Event for the Dedicated Cloud, Virtual Private Cloud, or Virtual Private Cloud OnDemand Services:

a) Any of the network interfaces of the Service Offering Network are unavailable for more than three (3) consecutive minutes. The "Service Offering Network" means the network that extends from the network interfaces of physical host servers for a class of service to the outside network interfaces providing the Service Offering's public internet connectivity.

b) The data store(s) associated with your block level storage for a class of service are unavailable for more than three (3) consecutive minutes.

c) The self-service console, cannot successfully authenticate a simulated user for more than five (5) consecutive minutes.

d) Your running virtual machines for a class of service become inaccessible for more than five (5) consecutive minutes due to physical host server failures.

2. Each of the following will be considered an SLA Event for the Data Protection Service:

a) The backup storage repository associated with your Data Protection service is unavailable for more than three (3) consecutive minutes.

b) The start time associated with your backup scheduling window is missed for longer than thirty (30) consecutive minutes.

c) The standard 24-hour recovery point objective (RPO) is missed for any virtual machines actively enrolled in the service.

d) Any restore operation for a virtual machine fails to complete due to backup infrastructure failures.

3. Each of the following will be considered an SLA Event for the Disaster Recovery Service:

a) Any of the network interfaces of the Service Offering Network are unavailable for more than three (3) consecutive minutes.

b) The data store(s) associated with your block level storage for replication is unavailable for more than three (3) consecutive minutes.

c) The self-service console, cannot successfully authenticate a simulated user for more than five (5) consecutive minutes.

d) Your failed-over virtual machines for a class of service become inaccessible for more than five (5) consecutive minutes due to physical host server failures.

e) Any built-in service functions for failover testing, planned migration, or live failover and recovery result in virtual machine replicas not powering on in less than 4 consecutive hours from the time a request is acknowledged and approved by VMware.

4. The following will be considered an SLA Event for the Object Storage service:

a) A more than five (5) percent Error Rate for more than ten (10) consecutive minutes – where "Error Rate" means the number of valid requests that result in a response with HTTP Status 500 and Code "Internal Error" divided by the total number of valid requests during each five-minute period.

SaaS – VMware AirWatch

AirWatch warrants it will provide Availability of the Hosted Services 99.9% of the calendar month (the "Service Level"). To the extent that the Hosted Services fail to conform to the Service Level, Customer may request service credits ("Outage Credits") as provided herein. A failure or lack of Availability for any period of time of at least one minute during which Customer is unable to utilize the Hosted Services due to AirWatch's failure to provide Customer with the specified services constitutes an "Outage". All Outage measurements will be rounded up or down to the nearest one minute increment, with increments equal to or greater than 30 seconds being rounded up to the next minute. Outage Credits are based on cumulative periods of Outage over a calendar month. Final determinations of the length of the cumulative periods of Outage over a calendar month shall be based on AirWatch's internal monitoring equipment and records. Outage Credits will be taken against only the Hosted Service fees for the month in which the Outage occurred. Outage Credits will be calculated in accordance with the following as outlined in **Table 37**.

Cumulative duration of Outage periods within a particular calendar month	Percentage of the Hosted Services fees to be credited as an Outage Credit
45 minutes through 3 hours, 36 minutes	10%
3 hours, 37 minutes through 7 hours, 12	20%
Greater than 7 hours, 12 minutes	30%

Table 37. vCloud Government Service SLAs

NOTE: All response times are based upon requests logged by phone only.

6.12.5 Describe the firm's procedures and schedules for any planned downtime. {8.12.5}

VMware Response:

VMware IaaS Services

Customers are notified in advance of any expected downtime with vCloud Air services. Planned downtime is scheduled for off peak hours to minimize customer impact. Generally, our goal is to keep planned downtime to a cumulative monthly maximum is 21 minutes 54.9 seconds for vCloud Air and 43 minutes 49.7 seconds for vCloud Government Service. Customers are notified immediately upon completion of the planned downtime. Planned downtime accounts for the time that would be required to roll back any maintenance changes in the event that maintenance proves unsuccessful. This mitigates the risk of extended planned downtime. In the event that rollback occurs, the maintenance plan and patches will be reviewed and modified to ensure success of a subsequent planned outage.

VMware AirWatch

AirWatch shall provide at least five (5) days' advance notice via email of Maintenance Windows or if, under the circumstances, five (5) days' notice is not practical, AirWatch shall provide as much advance notice via email as is reasonably possible. AirWatch does not have published maintenance windows; we provide upgrades to environments and patches according to release schedules to minimize downtime. Our goal is to keep maintenance windows to 8 cumulative hours per month for all activities.

6.12.6 Describe the consequences/SLA remedies if disaster recovery metrics are not met. {8.12.6}

VMware Response:

VMware IaaS Services

Please refer to section 6.12.4 for VMware's consequences and remedies if an SLA is not met.

VMWare AirWatch

We have detailed recovery procedures that include defined steps, roles and responsibilities and accountable personnel to help ensure streamlined disaster recovery.

As conversations progress, AirWatch can provide specific details regarding our disaster recovery timelines and strategies.

6.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics. {8.12.7}

VMware IaaS Services

VMware vCloud Air provides Web-based capacity reporting via the MyVMware portal. For detailed performance reporting, participating entities may wish to acquire VMware vRealize Operations suite, which is a non-Web based software product which provides real-time and historic performance statistics for vCloud Air.

VMware AirWatch

We can provide sample performance testing documents that validate our ability to handle anticipated workload under real-world conditions as conversations progress.

We have a dedicated team for scalability and performance testing. They work with both internal teams and customers to conduct testing.

6.12.8 Ability to print historical, statistical, and usage reports locally. {8.12.8}

VMware Response:

VMware IaaS Services

At the present time, VMware does not provide end user customers with specific reports for SLA performance. VMware tracks the overall health of the environment and will report to customers in the event of an outage. However, specific SLA performance is not delivered as a report, but as an alert. It is currently the customer's responsibility to track downtime within their environments and report to VMware when they believe SLA has been violated.

VMWare AirWatch

Customers can export and print solution data using interactive dashboards (CSV), reports (PDF, XLS, and CSV), the AirWatch Hub (PDF), and event log (CSV).

6.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365. {8.12.9}

VMware Response:

VMWare IaaS Services

VMware vCloud Air and vCGS Operations personnel monitor the cloud environments 24x7x365 to help ensure the confidentiality, integrity, and availability of our IaaS Services.

VMware vCloud Air and vCGS includes the following support for all IaaS offerings:

- One support team for business and technical assistance
- 24x7 support for Severity 1 issues
- Fast response times for critical issues
- Unlimited number of Support Requests
- Access to documentation and technical resources, Knowledge Base, discussion forums

VMware AirWatch

AirWatch Cloud Operations personnel monitor the cloud environment 24x7x365 to help ensure the confidentiality, integrity, and availability of our hosted offering. All Support Service levels include 24/7/365 support for severity 1 incidents, and continues service request work based on 24/7 customer access and interaction.

6.12.10 Offeror must describe its scale-up and scale-down, and whether it is available 24x365. {8.12.10}

VMware Response:

VMWare IaaS Services

Details on the rapid elasticity capability of each VMware vCloud Air and vCGS offering are provided in section 6.2. These capabilities are available 24x7 to users.

VMware AirWatch

Designed to easily support any mobile deployment, from 10 to tens of thousands of devices, the AirWatch platform is highly scalable. This allows you to support an unlimited number of devices without sacrificing management capabilities. AirWatch application servers are stateless by design and operate behind a network load balancer for instant and infinite horizontal scaling. These features help to reduce the upfront investment cost and allow for additional remote capacity when needed.

6.13 CLOUD SECURITY ALLIANCE {8.13} (E)

Describe your level of disclosure with CSA Star Registry for each Solution offered.

6.13.a Completion of a CSA STAR Self-Assessment, as described in Section 5.5.3. {8.13.a}

VMware Response:

VMware IaaS Services

VMware has completed Level 1 CSA STAR Registry Self-Assessment for vCloud Air and it was published on December 31, 2014. VMware has not completed the CSA STAR Registry Self-Assessment for it vCGS cloud offering.

VMWare AirWatch

While AirWatch has not registered with CSA STAR, we have completed a CAIQv3.0.1, which accompanies our response. Please note that some information has been redacted for open records purposes; AirWatch can provide additional details as conversations progress.

6.13.b Completion of Exhibits 1 and 2 to Attachment B.

VMware Response:

VMware IaaS Services

VMware has completed a CAIQv3.0.1 on December 30st, 2014. It is available on the CSA Star Registry website and included as **Appendix B**.

VMWare AirWatch

While AirWatch has not registered with CSA STAR, we have completed a CAIQv3.0.1 located in **Appendix B**, which accompanies our response.

6.13.c Completion of a CSA STAR Attestation, Certification, or Assessment.

VMware Response:

VMware IaaS Services

VMware has not completed and at the present time, this is not on VMware's roadmap for completion.

VMWare AirWatch

While AirWatch has not registered with CSA STAR, we have completed a CAIQv3.0.1, which accompanies our response. Please note that some information has been redacted for open records purposes; AirWatch can provide additional details as conversations progress.

6.13.d Completion CSA STAR Continuous Monitoring.

VMware Response:

VMWare IaaS Services

Not applicable. vCloud Air and vCGS are not STAR compliant; please refer to the provided CAIQ for related information.

VMware AirWatch

Not applicable. AirWatch is not STAR compliant; please refer to the provided CAIQ for related information.

6.14 SERVICE PROVISIONING {8.14} (E)

6.14.1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity. {8.14.1}

VMware Response:

VMware IaaS Services

vCloud Air OnDemand instances are instantiated immediately when requested by purchasing entities online. For services which require an initial purchase order, the following process applies.

Initial Order

Purchasing entities would contact the VMware NASPO contracts manager to request an expedited purchasing process. The contract manager will work directly with the engineering, sales, pricing, and contracts organizations to ensure that the order is processed in real time. The NASPO standard terms and conditions will expedite the contracts and legal review as they will have already been approved. If additional terms and conditions are required by the purchasing entity the VMware Contracts manager will ensure that they are reviewed and negotiated as promptly as possible. If distributors are used, the Program Manager will directly interface with each company in the supply chain to ensure that the order is processed immediately upon receipt by each party.

Increased capacity

OnDemand resources and prepaid resources with remaining capacity can be increased in real time via the online portal. Services which require additional purchases would follow the process above.

VMware AirWatch

Participating Agencies will work with the NASPO contracts manager to procure additional services for their AirWatch implementations. Customers can directly implement and update configurations through the AirWatch administrative console. Additionally, customers can submit support tickets for any solution issues that will be tracked through completion.

6.14.2 Describe in detail the standard lead-time for provisioning your Solutions. {8.14.2}

VMware Response:

VMware vCloud Air Services

VMware vCloud Air OnDemand services can be purchased and provisioned in minutes via the vCloud Air self-service portal. VMware vCloud Air services other than OnDemand are purchased via purchase order. Purchase orders are typically processed on the day of order. Once services have been purchased the user can immediately begin provisioning services from the self-service portal. These services are available within minutes of launch.

VMware vCloud Government Services

VMware vCloud Government Services are purchased via purchase order. Purchase orders are typically processed on the day of order. New environments require an RSA token that is shipped

overnight for two-factor authentication. Once the user has their RSA token, they can begin to provision IaaS Services.

VMware AirWatch

AirWatch is committed to implementing the solution in a timely manner and we work closely with customers to meet internal deadlines.

Delivery and deployment models will vary depending the hosting model selected by the customer:

- SaaS deployments can be implemented within several days and some within a few hours
- Large enterprise deployments with numerous integration endpoints may require additional time

Once an order is placed, we immediately begin working with the customer to finalize terms and conditions in a mutually agreeable manner and begin the implementation process.

We schedule regular check-ins for project status updates and to discuss any questions or concerns.

6.15 BACK UP AND DISASTER PLAN {8.15} (E)

6.15.1 Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements. {8.15.1}

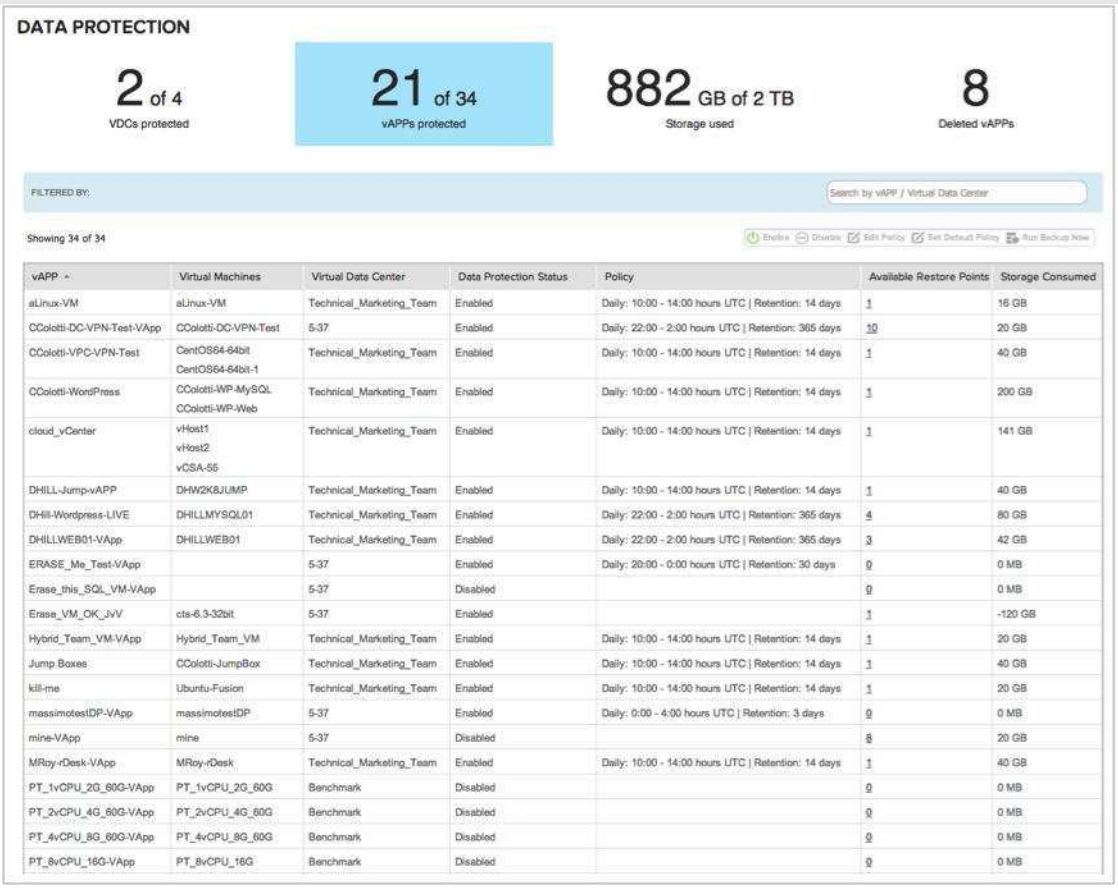
VMware Response:

VMware IaaS Services

We retain logs of the service for one full year for legal purposes. Our Data Privacy Addendum provided in **Appendix C** includes the following term for how we respond to a subpoena.

*"***Third Party Requests for Service Data.** *If a third party raises a complaint about or requests access to Service Data, we will attempt to redirect the third party to you. If we are required to respond to a subpoena, court order, warrant, audit or agency action and that occurrence demands that we disclose Service Data, we will promptly notify and provide you with a copy of the demand unless legally prohibited from doing so."*

In addition, Participating Entities that leverage VMware Data Protection are able to specify the retention period of their backups to comply with policies and legal requirements. Data Protection leverages snapshots to take an image level backup of virtual machines. When a backup is initiated, a snapshot is taken of that virtual machine. Once the snapshot is taken it is then stored on the Data Protection storage for the duration of the retention period assigned in the policy. The policy column in the screenshot below (**Figure 15**) illustrates the variety of data retention policies that have been set within a sample customer's vCloud Air Data Protection instance. In this example retention policies range from 3 to 365 days.



vAPP	Virtual Machines	Virtual Data Center	Data Protection Status	Policy	Available Restore Points	Storage Consumed
aLinux-VM	aLinux-VM	Technical_Marketing_Team	Enabled	Daily: 10:00 - 14:00 hours UTC | Retention: 14 days	1	16 GB
CColotti-DC-VPN-Test-VApp	CColotti-DC-VPN-Test	5-37	Enabled	Daily: 22:00 - 2:00 hours UTC | Retention: 365 days	10	20 GB
CColotti-VPC-VPN-Test	CentOS64-64bit CentOS64-64bit-1	Technical_Marketing_Team	Enabled	Daily: 10:00 - 14:00 hours UTC | Retention: 14 days	1	40 GB
CColotti-WordPress	CColotti-WP-MySQL CColotti-WP-Web	Technical_Marketing_Team	Enabled	Daily: 10:00 - 14:00 hours UTC | Retention: 14 days	1	200 GB
cloud_vCenter	vHost1 vHost2 vCSA-55	Technical_Marketing_Team	Enabled	Daily: 10:00 - 14:00 hours UTC | Retention: 14 days	1	141 GB
DHILL-Jump-vAPP	DHW2K8JUMP	Technical_Marketing_Team	Enabled	Daily: 10:00 - 14:00 hours UTC | Retention: 14 days	1	40 GB
DHill-Wordpress-LIVE	DHILLMYSQL01	Technical_Marketing_Team	Enabled	Daily: 22:00 - 2:00 hours UTC | Retention: 365 days	4	80 GB
DHILLWEB01-VApp	DHILLWEB01	Technical_Marketing_Team	Enabled	Daily: 22:00 - 2:00 hours UTC | Retention: 365 days	3	42 GB
ERASE_Me_Test-VApp		5-37	Enabled	Daily: 20:00 - 0:00 hours UTC | Retention: 30 days	0	0 MB
Erase_this_SQL_VM-VApp		5-37	Disabled		0	0 MB
Erase_VM_OK_JvV	cts-6.3-32bit	5-37	Enabled		1	-120 GB
Hybrid_Team_VM-VApp	Hybrid_Team_VM	Technical_Marketing_Team	Enabled	Daily: 10:00 - 14:00 hours UTC | Retention: 14 days	1	20 GB
Jump Boxes	CColotti-JumpBox	Technical_Marketing_Team	Enabled	Daily: 10:00 - 14:00 hours UTC | Retention: 14 days	1	40 GB
kill-me	Ubuntu-Fusion	Technical_Marketing_Team	Enabled	Daily: 10:00 - 14:00 hours UTC | Retention: 14 days	1	20 GB
massimotestDP-VApp	massimotestDP	5-37	Enabled	Daily: 0:00 - 4:00 hours UTC | Retention: 3 days	0	0 MB
mine-VApp	mine	5-37	Disabled		8	20 GB
MRoy-rDesk-VApp	MRoy-rDesk	Technical_Marketing_Team	Enabled	Daily: 10:00 - 14:00 hours UTC | Retention: 14 days	1	40 GB
PT_1vCPU_2G_60G-VApp	PT_1vCPU_2G_60G	Benchmark	Disabled		0	0 MB
PT_2vCPU_4G_60G-VApp	PT_2vCPU_4G_60G	Benchmark	Disabled		0	0 MB
PT_4vCPU_8G_60G-VApp	PT_4vCPU_8G_60G	Benchmark	Disabled		0	0 MB
PT_8vCPU_16G-VApp	PT_8vCPU_16G	Benchmark	Disabled		0	0 MB

Figure 15. VMware Data Back Up Retention Policies

VMware AirWatch

Customers can export and archive solution data using interactive dashboards (CSV), reports (PDF, XLS, and CSV), the AirWatch Hub (PDF), and event log (CSV). Customers in a Dedicated Cloud deployment can leverage a robust data mart.

6.15.2 Describe any known inherent disaster recovery risks and provide potential mitigation strategies. {8.15.2}

VMware Response:

VMware IaaS Services

Table 38 provides common inherent disaster recovery risks and potential mitigation strategies.

RISK	Unmitigated Probability	Mitigation	Mitigated Probability
Participating agency's lack of a disaster recovery plan leads to service outage or data loss in the event of a disaster.	High Risk	Participating Entities are encouraged to develop a disaster recovery plan to mitigate against service outage or data loss. In parallel, entities are encouraged to leverage VMware data protection, VMware Disaster Recovery, and other high availability services while a formal plan is written	No Risk

Participating entity chooses inappropriate data center location leading to service degradation or outage.	High Risk	Participating Entities are encouraged to choose datacenter(s) that is geographically proximate to their end users to maximize performance. In addition, location of disaster recovery data center should be geographically separated from primary data center.	Low Risk
Participating entity fails to budget for and acquire appropriate DR technology leading to inability to recover from disasters.	High Risk	Participating Entities are encouraged to include DR capabilities in their costs estimates for cloud deployments to ensure budget is available to acquire those services.	No Risk
Participating entity fails to ensure cloud service SLAs (e.g. RPO & RTO objectives) meet their mission requirements leading to inadequate service recovery times and data loss.	High Risk	Participating Entities are encouraged to review SLAs for each cloud service that they are interested in acquiring to ensure that they meet mission requirements. Care should also be taken to ensure service SLAs do not significantly exceed mission requirements to avoid unnecessary cost.	No Risk

Table 38. Disaster Recovery Risks

VMware AirWatch

Providing a secure and stable product that mitigates vulnerabilities, reduces risk and quickly responds to the evolving threat landscape is considered a top priority. Following the guidelines established in NIST SP 800-30, regular risk and vulnerability assessments are performed against the production environment to identify, assess and remediate emerging threats. When potential vulnerabilities are discovered, we follow a documented procedure to prioritize and deploy necessary patches.

- Vulnerabilities and threat-sources are identified by conducting interviews with various members of the Cloud Operations community and mapping data to the AirWatch business landscape.
- We can provide additional information as conversations progress.

6.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost. {8.15.3}

VMware Response:

VMware IaaS Services

VMware offers several technologies to provide redundancy, failover capability and the ability to run large scale applications independently in case one data center is lost.

vCloud Air is built upon infrastructure that is architected for High Availability leveraging proven vSphere High Availability (HA), vSphere vMotion, and VMware Distributed Resource Scheduler (DRS). These technologies allow Participating Entities to migrate live workloads and/or automatically restart VMs in the event of host maintenance or unexpected issues. These technologies also maintain a consistently high level of performance for all tenants.

VMware vSphere vMotion enables migration of live VMs to transfer your workloads during maintenance, without downtime. Unlike other cloud providers, VMware ensures that tenants are not impacted by standard maintenance. VMware performs vMotion migrations for maintenance behind the scenes for its tenants in vCloud Air during maintenance windows without disrupting tenant applications.

vMotion is also used to seamlessly migrate VMs from an on-premises environment to vCloud Air and back. Today, vCloud Air is one of only a few major cloud vendors that uses live migration to do maintenance. This capability will enable NASPO Participating Entities to perform live migrations to move their applications to and from the cloud for maintenance and other purposes. This technology inherently prevents the lock-in experienced when migrating to cloud services offered by others.

VMware Dynamic Resource Scheduler continuously monitors CPU and memory utilization across a cluster of vSphere hosts, allocating resources among VMs and rebalancing performance during high-volume peak times. This is performed 24x7 within the VMware vCloud Air environment.

VMware vSphere High Availability delivers the availability required by most applications running in VMs, independent of the operating system and application running in it. Whether Participating Entities leverage Microsoft Windows or Linux; off-the-shelf or custom developed application; single VMs or many, HA provides uniform, failover protection against hardware and operating system outages within vCloud Air.

HA can:

- Monitor VMware vSphere hosts and VMs to detect hardware and guest operating system failures.
- Restart VMs on other vSphere hosts in the cluster without manual intervention when a server outage is detected.
- Reduce application downtime by automatically restarting VMs upon detection of an operating system failure.

Other cloud providers require you to build availability in to your application. In the best case scenario, this is as simple as including a load balancer in front of multiple VMs in the same tier to achieve basic high availability.

However, often the technologies of other cloud service providers requires a complete redesign of the hosted application, and often network devices such as load balancers are offered at an additional cost, unlike vCloud Air.

vCloud Air was built to run hosted applications as-is, providing availability down to a single VM instance, and balancing resources across multiple tenant needs with DRS. Unlike other clouds, with vCloud Air and vCGS, Participating Entities are not required to rebuild their application to get the flexibility and agility that cloud can provide. Of course, vCloud Air customers usually do not just stop at moving applications to vCloud Air. Once in the cloud they start to explore features like our Advanced Networking Services and using APIs, automation, and CI/CD tools to deliver services faster. And, where it makes sense, customers do look at application redesigns as well, but with vCloud Air it is not because they must redesign to ensure the application is always available.

VMware AirWatch

AirWatch features active-passive configurations for high availability and redundancy with all components made to failover with minimal downtime. Load balancing capabilities are deployed across multiple data centers to ensure immediate server pick up, ensuring zero end user downtime. AirWatch also incorporates replication technology featuring SQL log shipping or network SAN byte replication to prevent data loss.

6.16 SOLUTION ADMINISTRATION {8.16} (E)

6.16.1 Ability of the Purchasing Entity to fully manage identity and user accounts. {8.16.1}

VMware Response:

VMware IaaS Services

VMware management infrastructure requires two-factor authentication and multiple layers of access control. vCloud Air customers have the ability to provide access to their designated users. User account management is maintained by the customer.

vCloud Air customers have the ability to provide access to their designated users. User account management is maintained by the customer.

VMware AirWatch

The Purchasing entity has the ability to fully manage identity and user accounts for administrators and end users through the web console. Customers can optionally integrate with AD/LDAP to inherit your existing structure and policies.

6.16.2 Ability to provide anti-virus protection, for data stores. {8.16.2}

VMware Response:

VMware IaaS Services

Anti-virus software is installed on all development, domain and production hardware devices owned and operated by VMware, which hold company data, passwords, or keys. These devices maintain the most recent version of the anti-virus software signature file.

VMware AirWatch

AirWatch has installed a best-in-class, continuously-updated anti-virus suite on servers in the SaaS environment

6.16.3 Ability to migrate all Purchasing Entity data, metadata, and usage data to a successor Cloud Hosting solution provider. {8.16.3}

VMware Response:

VMware IaaS Services

Customers can export their data and applications from vCloud Air, using either the vCloud Connector utility for over-the-network migrations or offline data transfer to move large quantities of data on disk via physical shipment.

VMware AirWatch

In the event that an AirWatch Cloud customer wishes to migrate to an "on-premise" solution hosted with a new cloud hosting provider, AirWatch will assist the customer in using solution controls to export data. Customers in a Dedicated Cloud deployment can leverage a robust datamart.

6.16.4 Ability to administer the solution in a distributed manner to different Participating Entities. {8.16.4}

VMware Response:

VMware IaaS Services

All customers have access to a self-service portal to consume and manage the cloud resources purchased from VMware. The service console allows cloud administrators to manage the virtual data center, configure network services and manage the virtual machine instance life cycle. The console is the central location for all self-service interactions with the service.

VMware AirWatch

Our multitenant architecture allows large enterprises to manage multiple device groups or entities uniquely from a single instance of the software.

6.16.5 Ability to apply a participating entity's defined administration polices in managing a solution. {8.16.5}

VMware Response:

VMware IaaS Services

VMware vCloud Air and vCloud Government Service allow customers to implement role based access controls. The following roles are provided. Participating Entities may assign their users to one or more roles according to their own administration policies.

- Account Administrator
- Virtual Infrastructure Administrator
- Network Administrator
- Read-Only Administrator
- End User

Furthermore, Participating Entities that wish to govern their IaaS services using software can do so via integrations with VMware and 3rd party tools. VMware vCloud Air and vCloud Government Service include APIs which enable integration of the services to management and automation tools such as VMware vRealize Automation, VMware vRealize Operations, and third party applications such as ITSM tool suites.

VMware AirWatch

Participating Entities can define administration policies for the console to best fit deployment needs. Optionally integrate with AD/LDAP to leverage your existing provisioning structure.

6.17 HOSTING AND PROVISIONING {8.17} (E)

6.17.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack. {8.17.1}

VMware Response:

VMware IaaS Services

Participating Entities can provision, manage and consume your hybrid cloud resources through the vCloud Air and vCGS Web consoles. The vCloud Air and vCGS consoles are the primary portal for access, consumption, and management of cloud resources purchased from VMware, including virtual data center management, configuration of network services, and virtual machine instance lifecycle management. The console also provides single sign-on access to the vCloud Director portal. In vCloud Director, administrators can perform advanced management of virtual data centers, and end users can perform advanced management of virtual machines.

Detailed processes for provisioning cloud hosting services for vCloud Air and vCloud Government Service are documented in the vCloud Air Getting Started and User Guides located within the vCloud Air Documentation center online. In addition to this documentation, free tutorials, hands-on labs, and a frequently asked questions repository is provided to the public at no cost.

VMware's vCloud Air and vCloud Government Service provisioning stack is built upon VMware's proven products including the VMware's vSphere Hypervisor, VMware NSX, and VMware vCloud Director. This underlying technology is abstracted from the user to simplify usability while still providing the powerful capabilities of the stack.

vCloud Air provides an interface that allows users to select from a catalog of pre-built OS images and allows them to provision on the fly.

Participating Entities may also be interested in building their own reusable blueprints to rapidly provision and de-provision complex IT systems. This can be done via VMware vRealize Automation which is described in detail in Section 6.16 above.

VMware AirWatch

AirWatch uses industry recognized tools and follow best practices to deploy, configure, and maintain server images. We do not apply customer-supplied templates and do not share templates with customers.

Our Information Security team identifies applicable security standards and the AirWatch Server Team creates a secure baseline image for deployment throughout the SaaS environment.

6.17.2 Provide tool sets at minimum for: {8.17.2}

6.17.2.1 Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.) {8.17.2.1}

VMware Response:

VMware IaaS Services

vCloud Air provides an interface that allows users to select from a catalog of pre-built OS images and allows them to provision on the fly.

vRealize Automation is the next level for provisioning, delivering, and managing IT services on VMware vSphere infrastructure as well as VMware vCloud Air all with a unified management experience. It provides governance and blueprints to deliver services from on premise into vCloud Air.

Customers can integrate vCloud Air with vRealize Automation. In this setup, users access vCloud Air primarily through the vRealize Automation service catalog which handles authentication to the service itself.

VMware AirWatch

AirWatch uses industry recognized tools and follow best practices to deploy, configure, and maintain server images. We do not apply customer-supplied templates and do not share templates with customers.

6.17.2.2 Creating and storing server images for future multiple deployments {8.17.2.2}

VMware Response:

VMware IaaS Services

We also allow for template and gold master images to be stored on-premise and deployed to the cloud. We also provide storage of templates and master images in vCloud Director catalogs in in vCloud Air to enable provisioning of more complex integrated systems.

VMware AirWatch

Our Information Security team identifies applicable security standards and the AirWatch Server Team creates a secure baseline image for deployment throughout the SaaS environment.

6.17.2.3 Securing additional storage space {8.17.2.3}

VMware Response:

VMware IaaS Services

Additional storage can be purchased and provisioned in 48 hours.

VMware AirWatch

Our Information Security team identifies applicable security standards and the AirWatch Server Team creates a secure baseline image for deployment throughout the SaaS environment.

6.17.2.4 Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources). {8.17.2.4}

VMware Response:

VMware IaaS Services

The vCloud Air infrastructure, including the top layer management stack, the customer management stack and the computing/storage/network hardware are monitored for availability, capacity and performance. Customers are responsible for monitoring their own VMs (OS, apps). Customers can use on premise monitoring tools to manage and monitor their applications and OSes over VPN and direct connect.

VMware AirWatch

The AirWatch Cloud Operations team monitors the SaaS environment. AirWatch follows the Fault, Configuration, Accounting, Performance, and Security (FCAPS) model to monitor the SaaS environment.

Because the solution is built on industry-standard ASP.NET architecture, it integrates into existing management and monitoring tools. Administrators can configure log data storage to destinations such as Windows Event Viewer, SNMP traps, syslog, SMTP email alerts, etc. The solution also integrates directly with Microsoft SCCM.

The communication layer includes a complete infrastructure for API integration to third parties as well as a rich set of existing APIs, web services, single sign on and authentication protocols.

Integrate with security information and event management (SIEM) solutions for enhanced logging of events occurring in the console. Administrators can view events, filter by event type, category and module, and export events. Event logging settings can be configured based on severity levels, with the ability to send specific levels to external system via syslog integration.

6.18 TRIAL AND TESTING PERIODS (PRE- AND POST- PURCHASE) {8.18} (E)

6.18.1 Describe your testing and training periods that your offer for your service offerings. {8.18.1}

VMware Response:

VMware IaaS Services

VMware offers a variety of testing and training periods with its service offerings. Trials and testing periods can be arranged for a 30-day period.

In addition, VMware offers Hands-on Labs which provide customers with a no-cost environment which enables them to use the vCloud Air Services themselves. VMware Hands-on labs are self-paced labs which allow customers to try vCloud Air's powerful virtual machines features—including workload migration, cloud management, and networking. With Hands-on Labs, Participating Entities can get a lab up and running in minutes with full technical capabilities, without installing anything new on modifying their existing hardware. For example, the following hands-on labs will allow Participating Entities to experience vCloud Air Administration and vCloud Air Disaster recovery.

- Jump Start for vSphere Admins: Provides an overview of vCloud Air, walks you through the service, explains the architecture and consumption principles, along with some basic networking.
- Disaster Recovery: Learn how to leverage vCloud Air as a Disaster Recovery target. Failover, reverse failback, point-in-time recovery, automate with vRealize Orchestrator, all using your vSphere Web Client.

These publicly accessible labs can be accessed via the Internet 24 hours a day, 7 days a week.

VMware AirWatch

We encourage the use of our Free Trial as part of customer acceptance strategy

Our Free Trial enables you to review all solution functionality.

- Enroll any of the device types we support, including, Android, Apple, Windows and BlackBerry.
- Access the complete feature set and leverage our full array of web APIs
- Explore trial guides and live training webinars.
- Use our expansive customer tools and resources, including training materials, user guides, getting started guides, etc.

Testing Upgrades – We offer two options for user acceptance testing (UAT): a "sandbox" environment and a dedicated environment.

- UAT Sandbox – Create individual or combined sandboxes for UAT users within a single AirWatch environment, leveraging the multitenancy of the solution.
- UAT Environment – Create a new cloud environment solely for UAT, independent of the production environment and using dedicated hardware and software.

UAT sandboxes and environments are scoped and priced separately.

6.18.2 Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements. {8.18.2}

VMware Response:

Please see response to question 8.18.1 above.

6.18.3 Offeror must describe what training and support it provides at no additional cost. {8.18.3}

VMware Response:

In addition to the hands on labs described in section 8.18.1 above, VMware provides a variety of computer based training in the form of documentation and online videos at no cost.

For details on support please see our responses to questions 8.3.3, 8.4, and 8.12.10 above.

6.19 INTEGRATION AND CUSTOMIZATION {8.19} (E)

6.19.1 Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations. {8.19.1}

VMware Response:

Please refer to section 6.19.2 below for details on how VMware solutions can be integrated into other complementary applications.

6.19.2 Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities. {8.19.2}

VMware Response:

VMware IaaS Services

One of VMware's valuable differentiators is the extent to which its products integrate and interoperate. For example, Participating Entities that have an existing investment in VMware vSphere, vRealize Automation, and/or vRealize Operations (or those interested in investing in them) can use these tools to manage, automate, and operate their vCloud Air and vCGS workloads from a single pane of glass.

NASPO Participating Entities can leverage existing infrastructure investments, processes, and workforce expertise in VMware management and automation tools to complement their vCloud Air experience. The hybrid cloud management solutions from VMware integrates a variety of familiar tools with vCloud Air to provide full control of investments. Participating Entities can increase productivity and ROI by extending their vSphere data center to vCloud Air, using a common management approach that enables consistent and automated delivery of IT services both on- and off-premises.

vCloud Air Web Portal

Participating Entities can use the vCloud Air Web Portal to manage their vCloud Air infrastructure. They will get advanced control of their environments, including detailed views of allocated and consumed resources by environment and VDC. They also have the ability to set up and control virtual machines and user management access rules, establish network settings, and more. All actions are carried out in real time and are reflected in other portals. If entities also need to manage content in their existing data center, they can use the vSphere Client Plug-in for a true "single pane of glass" experience. **Figure 16** provides an image of the portal.

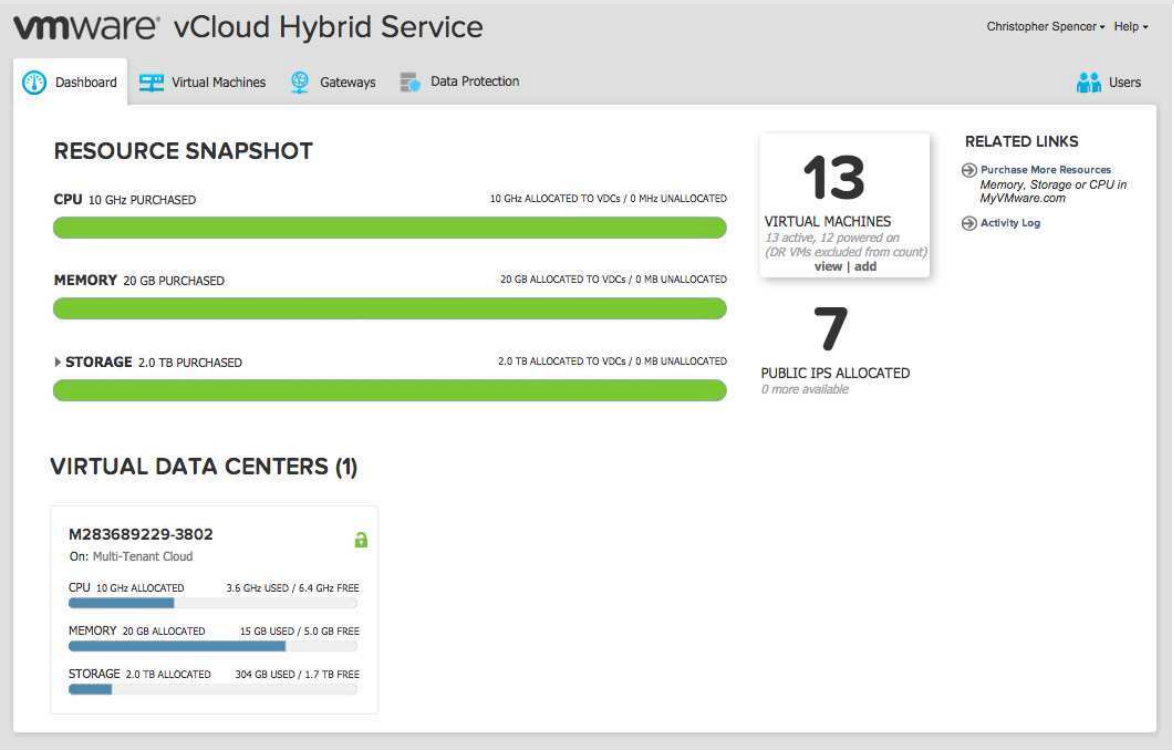


Figure 16. vCloud Air Web Portal

vSphere Web Client Plug-in

In addition to offering a client plug-in for the vSphere client, VMware also offers a plugin to manage resources onsite and offsite from the vSphere Web Client from a "single pane of glass." With vCloud Air vSphere Client Plug-in, Participating Entities can view and administer resources onsite as well as on vCloud Air from the vSphere Client version 5.5 and later. This web client interface provides an additional portal experience, in addition to the dedicated vCloud Air Portal, for the administrator to get the best experience possible in an easy-to-use interface inside vSphere. Please refer to **Figure 17** for an image of the portal.

The plug-in offers:

- Support for vCloud Air Dedicated Cloud, Virtual Private Cloud, and Disaster Recovery, including visibility into the resources for these VMs and VDCs
- Management controls for these VMs, including visibility of Compute, Memory, Storage, and Storage Tiers, allowing you to view and manage these resources, including specifying additional storage

Figure 17. vCloud Air vSphere Client Plug-in

vRealize Automation

Participating Entities can automate the end-to-end delivery and management of infrastructure and applications with vRealize Automation (previously known as vCloud Automation Center or vCAC). Out-of-the-box vRealize Automation versions 5.2 and 6.0 are now fully certified on vCloud Air. Entities can use the self-service portal in vRealize Automation to create service catalogs, reserve resources such as CPU, memory, and network, and provide role-based rights to user groups on vCloud Air.

vRealize Automation Enterprise Edition also offers advanced application services capabilities (formerly found in Application Director) that include the ability to create application blueprints to describe application deployment topologies on vCloud Air. Now you can utilize pre-built logical templates, services, and application components to assemble Application Blueprints on vCloud Air, all from within the private data center.

vRealize Operations Manager

Participating entitles may extend the capabilities of vRealize Operations Manager to vCloud Air with a Management Pack. The vRealize Operations Management pack for vCloud Air includes an embedded adapter that collects metrics, change events, and resource topology information from vCloud Air.

By monitoring workloads running across clouds with vRealize Operations Manager, you can:

- Consolidate: View both onsite and cloud workloads
- Isolate: Resolve performance bottlenecks fast by working with vRealize Operations capabilities that are already in use today
- Contain: Avoid the cost of a second operations team to manage cloud infrastructure or applications.

VMware AirWatch

Our advanced integration enables you to preserve your investment in existing enterprise resources, centralize mobility management and streamline user enablement.

- Integrate with directory services for end user authentication and group structure
- Use your existing certificate and PKI investments to provide secure authentication to corporate resources
- Leverage existing email infrastructures such as Exchange, Office 365 and more
- Integrate with corporate networks to enable secure access to Wi-Fi and VPN
- Use existing monitoring systems to track device and console events or monitor your on-premises EMM infrastructure

Access our collection of APIs that allow external programs to use core product functionality and data to integrate with existing IT infrastructures and third-party applications

- Available web services include user enrollment, device registration, device groups, user information, device data, search functions, custom attributes, remote device commands and bulk actions, device and system events and notifications, application groups, VPP management, product provisioning, tags, and other systems management and operation information.

AirWatch is recognized as a global leader in mobile security and enterprise mobility management, with more than 16,000 customers and 2,000 global associates. Our large customer base, combined with a research and development team of 600+, allows AirWatch to provide the broad functionality at a low cost. The AirWatch platform features industry-leading mobile device, email, application, content and browser management solutions. Whether enabling a Bring Your Own Device (BYOD) program or corporate-owned and line-of-business devices, organizations can implement these solutions standalone, in a dual persona containerized solution or as a comprehensive platform based on device type, use case and user role in the organization.

Customers can also use granular configuration settings in the console to assign content, apps, restrictions, etc. to device across the fleet. Use built-in customization features to brand or white-label the web console, Self-Service Portal and AirWatch Catalog at the global level or by group, with additional app branding options through the AirWatch Software Development Kit.

6.20 MARKETING PLAN {8.20} E)

Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities. {8.20}

VMware Response:

VMware IaaS Services

To maximize utilization of the contract, we have created a comprehensive sales and marketing plan. Elements of our plan include: selecting in-state resellers for enablement and fulfilment, trade show participation across the US, targeted cloud-based use cases to share with potential customers, and training plan for VMware and resellers. Please see **Appendix E** for the VMware Marketing Plan.

6.21 RELATED VALUE-ADDED SERVICES TO CLOUD SOLUTIONS {8.21} (E)

Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services. {8.21}

VMware Response:

We are pleased to offer the following valued added services to Utah and all other Participating Entities.

Professional Services

VMware and AirWatch Professional Services offers an array of consulting services to assist agencies and organizations with evaluating their options to move applications to the cloud. Provided below are a few examples of the VMware and AirWatch Cloud Consulting Services.

VMware Cloud Assessment Service

The objective of this engagement is to assist Customer with driving alignment and momentum to accelerate Customer's ability to take advantage of VMware's Hybrid Cloud solutions. To achieve this objective VMware will:

- Assess Customer's current goals, objectives and challenges with moving to a Hybrid Cloud model
- Assess the key use cases and benefits expected relative to Hybrid Cloud
- Assess the results of a limited, current state review of the network and an agreed application to determine Hybrid Cloud feasibility
- Provide a Future State Hybrid Cloud Vision Diagram and Implementation Roadmap aligned to the prioritized use cases, including VMware's finding, considerations and recommendations

VMware vCloud Air Accelerator Service

The VMware vCloud Air Accelerator Service assists customers with extending their private VMware vSphere environment to a VMware vCloud Air public cloud. This Accelerator Service engagement incorporates VMware recommended best practices in a practical design that is targeting non-production workloads such as a test, development or other non-production environments. The benefits that customers will obtain from this service include:

- Understand key features, design options, and configuration best practices for your new vCloud Air environment.
- Learn operational and technical best practices for linking on-premises vSphere environments and off-premises vCloud Air public cloud environments.
- Optimize infrastructure virtualization and improve VM workload management with the integration of vCloud Air into your infrastructure strategy.

VMware vCloud Air Disaster Recovery Accelerator Service

Customer wants to proactively plan for the continued computing operations of its agency as part of its strategic business continuity and disaster recovery initiative. The VMware vCloud Air Disaster Recovery Accelerator Service provides a non-production design, deployment and validation of a disaster recovery solution for business applications to be recovered to vCloud Air in the event of a primary site failure.

The architectural design is developed to support business continuity and disaster recovery of non-production workloads. The implementation and configuration is conducted jointly with Customer team members to enhance the learning experience during the design and deployment of the solution.

The primary objective of this service is to implement a disaster recovery solution using VMware vSphere, VMware vCloud Air Disaster Recovery and VMware vSphere Replication according to a documented architecture that can be successfully implemented and validated in the Customer environment in preparation to protecting production workloads.

Secondary objectives include providing a disaster recovery solution overview and knowledge transfer so that Customer understand the workload considerations for protecting workloads with disaster recovery and also how to integrate with automation tools to provide efficient failover and failback processes.

VMware Migration Assessment Service

Since the introduction of virtualization over a decade ago, organizations have wanted to relocate applications and data assets from legacy platforms to new platforms. Several application relocation tools were developed over that time; but the challenge to a successful migration is in the logistics of what to migrate when, how long an outage will be, is an outage acceptable, what tool is appropriate, can it be rolled back, and what's the impact to costs and services during the migration. As with the majority of large projects; the secret of success is in the level of planning performed before the project begins.

With the addition of VMware vCloud Air public cloud as a target for relocation, some additional considerations must be included in the process. Opportunities exist to optimize the applications migrated to the cloud. This might involve rework that ranges from basic repackaging for deployment through moderate refactoring, to complete redevelopment in selected cases. These changes can bring benefits, such as cloud portability and scaling, which might form part of the expected business value of migrating to cloud services.

The VMware Migration Assessment Service provides the foundation for an organization to successfully migrate operating system instances (referred to as OSIs) from a source platform to a target platform, and identifies applications that can benefit from degrees of rework. This service uses a combination of expertise in performance and capacity data interpretation, with a standardized process and with specialized tools, to deliver a detailed migration plan and a VMware Cloud Migration Portal configuration file.

Statement of Work Based Deliverables and Projects

In addition to the cloud assessments listed above, VMware can work with a customer to perform statement of work (SOW)-based engagements that incorporate specific customer deliverables. These engagement can be customized to meet the specific objectives of the customer.

6.22 SUPPORTING INFRASTRUCTURE {8.22} (E)

6.22.1 Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models. {8.22.1}

VMware Response:

VMware IaaS Services

VMware does not require the installation of new infrastructure as a prerequisite for consuming the cloud services described in this proposal.

VMware will provide the following value added Provisioning Services to participating entities:

- Implementation of platform components (physical servers, physical storage, and physical network devices) needed to support contracted resource pools when applicable.
- Providing initial network resources including default Public IP addresses when applicable.
- Providing initial resource pools (memory, processing, primary storage, and networking) when applicable.
- Creating the initial administrative user account in the Console using default administrator privileges and system preferences.

Participating entities will be responsible for the following provisioning services:

- Creating user accounts in the vCloud Air Console, and changing default system preferences as needed.
- Creating and configuring applicable Virtual Data Centers, vApps, VMs, and Networks using deployment templates and wizards.
- Installing and configuring custom or third party applications and operating systems on deployed Virtual Machines.
- If desired, deploying and maintaining on-premises deployments of vSphere Replication for use with Disaster Recovery, including but not limited to: installation of vSphere Replication, registering your local vSphere environment(s) with vCloud Air, selecting virtual machines for protection, and assigning a Recovery Point Objective (RPO) for replication frequency.

When deploying on VMware cloud services, we assume that the customer is already virtualized on VMware vSphere technology (or will do so prior to migrating applications). The VMware architects, provision, monitor and manage the vCloud Air Service infrastructure and surrounding components.

VMWare AirWatch

AirWatch provides, configures and maintains hosting equipment for SaaS customers. Customers maintain on-premise systems (i.e., Active Directory). We leverage best-in-class technology including Cisco, Dell, EMC, F5, Riverbed and VMware, to ensure high performance and data security.

6.22.2 If required, who will be responsible for installation of new infrastructure and who will incur those costs? {8.22.2}

VMware Response:

VMware IaaS Services

VMware does not require the installation of new infrastructure as a prerequisite for consuming the cloud services described in this proposal. If the customer needs to update any infrastructure in their data center to become "cloud ready", those costs are the responsibility of the customer.

For a fee, customer may also contract with VMware to provide professional services to assist agencies and organizations with evaluating their options to move applications to the cloud.

VMWare AirWatch

The solution is available in both a shared-hosted and dedicated-hosted environment and is easily accessible over the Internet. In one single instance of the software, we are able to deliver a secure and scalable solution comparable to an on-premise deployment. As an AirWatch Cloud customer, you will pay a monthly subscription fee for each device under management, which includes maintenance and system upgrades. You also have the flexibility to transfer to an on-premise deployment at any time.

6.23 ALIGNMENT OF CLOUD COMPUTING REFERENCE ARCHITECTURE {8.23} (E)

Clarify how your architecture compares to the NIST Cloud Computing Reference Architecture, in particular, to describe how they align with the three domains e.g. Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

VMware Response:

VMware IaaS Services

Cloud Air is an Infrastructure-as-a-Service offering based on vSphere, vCloud Director, and VMware networking solutions, including NSX. As aligned with the NIST definition of IaaS, vCloud Air delivers an on-demand self-service access to resources with broad network access, elasticity, and consumption-based metering.

See section 6.1 for a detailed discussion outlining how each proposed service meets the NIST essential characteristics of cloud computing.

VMware AirWatch

AirWatch partners with co-located and cloud-hosted Tier III data centers to support of SaaS offering.

We can provide sample deployments as under NDA to Participating Entities during task order negotiations as required.

Section 7 Confidential Protected, or Proprietary Information

Section Title: Confidential, Protected or Proprietary Information. All confidential, protected or proprietary Information must be included in this section of proposal response. Do not incorporate protected information throughout the Proposal. Rather, provide a reference in the proposal response directing Lead State to the specific area of this protected Information section.

If there is no protected information, write "None" in this section.

Failure to comply with this Section and Section 3.13 of the RFP releases the Lead State, NASPO ValuePoint, and Participating Entities from any obligation or liability arising from the inadvertent release of Offeror information.

3.13 Confidential or Proprietary Information

The Government Records Access and Management Act (GRAMA), UCA § 63G-2-305, provides in part that:

the following records are protected if properly classified by a government entity:

(1) trade secrets as defined in Section 13-24-2, the Utah Uniform Trade Secrets Act, if the person submitting the trade secret has provided the governmental entity with the information specified in UCA § 63G-2-309 (Business Confidentiality Claims);

(2) commercial information or non-individual financial information obtained from a person if:

(a) disclosure of the information could reasonably be expected to result in unfair competitive injury to the person submitting the information or would impair the ability of the governmental entity to obtain necessary information in the future;

(b) the person submitting the information has a greater interest in prohibiting access than the public in obtaining access; and

(c) the person submitting the information has provided the governmental entity with the information specified in UCA § 63G-2-309;

* * * * *

(6) records, the disclosure of which would impair governmental procurement proceedings or give an unfair advantage to any person proposing to enter into a contract or agreement with a governmental entity, except, subject to Subsections (1) and (2), that this Subsection (6) does not restrict the right of a person to have access to, after the contract or grant has been awarded and signed by all parties, ...

Pricing may not be classified as confidential or protected and will be considered public information after award of the contract.

Process for Requesting Non-Disclosure: Any Offeror requesting that a record be protected shall include with the proposal a Claim of Business Confidentiality. To protect information under a Claim of Business Confidentiality, the Offeror must complete the Claim of Business Confidentiality form with the following information:

1. Provide a written Claim of Business Confidentiality at the time the information (proposal) is provided to the state, and

2. Include a concise statement of reasons supporting the claim of business confidentiality (UCA § 63G-2-309(1)).

3. Submit an electronic "redacted" (excluding protected information) copy of the record. The redacted copy must clearly be marked "Redacted Version."

The Claim of Business Confidentiality Form may be accessed at:

http://www.purchasing.utah.gov/contract/documents/confidentialityclaimform.doc

An entire proposal cannot be identified as "PROTECTED", "CONFIDENTIAL" or "PROPRIETARY", and if so identified, shall be considered non-responsive unless the Offeror removes the designation.

Redacted Copy: If an Offeror submits a proposal that contains information claimed to be business confidential or protected information, the Offeror must submit two separate proposals: one redacted version for public release, with all protected business confidential information either blacked-out or removed, clearly marked as "Redacted Version"; and one non-redacted version for evaluation purposes, clearly marked as "Protected Business Confidential."

The Lead State and NASPO ValuePoint are not liable or responsible for the disclosure of any confidential or proprietary information if the Offeror fails to follow the instructions of this section.

VMware Response:

VMware's response does not include any confidential or proprietary information.

Section 8 Exceptions and / or Additions to the Standard Terms and Conditions

The VMware Point of Contact for negotiations is:

Karin Whitwood, Contracts Manager: kwhitwood@vmware.com, 571-375-3481 (office)

VMware has read agrees to the terms of the final RFP #CH16012, dated February 10, 2016 and has no exceptions or modifications to the final RFP language, excluding the Attachment A – Master Agreement.

VMware has identified Master Agreement provisions to which we noted our exception in a chart found in **Appendix A** of this proposal response. VMware believes that the revisions and additions presented in Appendix A reflect the applicable commercial industry standards and government requirements for the circumstances of the orders and services contemplated, as provided in the explanatory rationale.

Additionally, VMware has identified terms and conditions within Attachment A "Master Agreement Terms and Conditions final" that are included below, not as an exception but rather as an assumption or clarification of our understanding of the intent of the language. These assumptions are provided to avoid confusion and allow the opportunity for discussions to ensure mutual understanding.

Assumptions and Clarifications:

Section 2. Definitions – Data: VMware identified multiple data definitions throughout the Master Agreement, referenced with a lowercase "d" with regard to Contractor and other data. Accordingly, we understand and assume that the referenced used throughout are the applicable definitions rather than one singe definition.

Section 2. Definitions – Software as a Service (SaaS): VMware understands and assumes that the use of the word "consumer" in this case means the Participating or Purchasing Entity.

Section 19.f. Ordering: VMware noticed an unidentified term "Participating State contract" which we assume means "Participating Addendum."

Section 20 a.-d. Participants and Scope: VMware assumes that where Utah/NASPO refers to "Services" that "Services" also includes products. Additionally, that an Order would need to occur in addition to a Participating Addendum before the Contractor could provide Services (or products).

Section 31.c. Warranty: In subsection c. this appears to be an incomplete sentence. Please clarify the intent.

Section 9 Cost Proposal {Separate Volume}

Given that technology products generally depreciate over time and go through typical product lifecycles, it is more favorable for Purchasing Entities to have the Master Agreement be based on minimum discounts off the Offeror's' commercially published pricelists versus fixed pricing. In addition, Offerors will have the ability to update and refresh their respective price books, as long as the agreed-upon discounts are fixed. Minimum guaranteed contract discounts do not preclude an Offeror and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.

Offeror must identify its cost proposal, Attachment G, as "Cost Proposal – CH16012 Cloud solutions". No specific format is required for an Offeror's price schedule; however the Offeror must provide and list a discount from its pricing catalog. New discount levels may be offered for new services that become available during the term of the Master Agreement, as allowed by the Lead State.

Pricing catalogs should include the price structures of the cloud solutions models and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing must be all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.

The Lead State understands that each Offeror may have its own pricing models and schedules for the Services described in the RFP. It is the intent to of the RFP to allow price schedules that are viewed in the traditional line item structure or price schedule that have pay-as-you-go characteristics.

An Offeror's price catalog should be clear and readable. Participating Entities, in reviewing an Offeror's Master Agreement, will take into account the discount offered by the Offeror along with the transparent, publicly available, up-to-date pricing and tools that will allow customers to evaluate their pricing.

Individual Participating Addendums will use the cost proposals pricing as a base and may negotiate an adjusted rate.

Offeror's price catalog should be broken into category for each service category. For example if an Offeror provides a SaaS offering then its price catalog should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc.

Some Participating Entities may desire to use an Offeror for other related application modifications to optimize or deploy cloud solutions applications. Responses to the RFP must include hourly rates by job specialty for use by Participating Entities for these types of database/application administration, systems engineering & configuration services and consulting throughout the contract period. The hourly rates should be a fully burdened rate that includes labor, overhead, and any other costs related to the service. The specific rate (within a range) charged for each proposed contracted service would be the lowest rate shown unless justified in writing and approved by the Lead State. Any of these valued-added services must be included in your cost proposal, e.g., by an hourly rate.

Cost will be evaluated independently from the Mandatory Minimum Requirements, and the Technical responses. Inclusion of any cost or pricing data within the Detailed Technical Proposal will result in the proposal being judged as non-responsive for violation of UCA § 63G-6a-707(5).

All costs incurred by an Offeror in the preparation and submission of a proposal, including any costs incurred during interviews, oral presentations, and/or product demonstrations are the responsibility of the Offeror and will not be reimbursed by the Lead State or NASPO ValuePoint.

VMware Response:

Please see **Cost Proposal –CH16012 Cloud Solutions** for VMware pricing. This file is uploaded separately.

Attachment A: NASPO ValuePoint Master Agreement

VMware Response:

VMware has read and acknowledges.

Attachment B: Explanation Cloud Security Alliance Questionnaires

Exhibit 1 to Attachment B: Consensus Assessments Initiative Questionnaire

VMware Response:

Please refer to files Appendix B - VMware CAIQ#1 and Appendix B – VMware CAIQ#2 for VMware's completed response. These files have been uploaded separately.

Exhibit 2 to Attachment B: Cloud Controls Matrix

VMware Response:

VMware has only provided Exhibit 1 to Attachment B (CAIQ) within our response. As stated in section 5.5.3 of the RFP, vendors may submit either the CAIQ or CCM, or both.

Attachment C: NIST Service Models

VMware Response:

VMware has read and acknowledges. Please refer to section 6.1.4.a of our response for our affirmation of our willingness to comply with RFP CH16012 **Attachment C**.

Attachment D: Scope of Services

VMware Response:

VMware has read and acknowledges. Please refer to section 6.1.4.b of our response for our affirmation of our willingness to comply with RFP CH16012 **Attachment D**.

Attachment E: Intent to Participate & State-Specific Terms and Conditions

VMware Response:

VMware has received and acknowledges the state-specific terms and conditions provided in the RFP CH16012 **Attachment E**. If awarded a master agreement, VMware will undertake negotiations with the specific states regarding these terms and conditions.

Attachment F: Intentionally Removed

Attachment G: Cost Proposal Form (Separate Volume)

VMware Response:

Please see file: **Cost Proposal –CH16012 Cloud Solutions**. This file was uploaded separately.

Attachment H: Identification of Service Models

VMware Response:

Please refer to Attachment H – Identification of Service Models. This file was uploaded separately.

Appendix A – Exception and/or Additions to the Standard Terms and Conditions

VMware Response:

The VMware Point of Contact for negotiations is:

Karin Whitwood, Contracts Manager: kwhitwood@vmware.com, 571-375-3481 (office)

VMware has prepared an exceptions/clarification chart provided below in accordance with the specifications provided in this RFP CH16012, section 3.4 to include detail in suggested alternate language and rationale for the change presented. VMware respectfully reserves the right to negotiate the terms and conditions of the Master Agreement as provided in the solicitation to appropriately reflect applicable commercial industry standards and government requirements for the circumstances of the Solutions included. We are confident that we can reach a mutually agreeable agreement as we have in previous situations with public sector entities.

Please refer to Appendix A – VMware Exceptions, for a list of our proposed exceptions to the terms and conditions. This file has been uploaded separately.

Appendix B – CSA STAR Assessment

VMware Response:

Please refer to files Appendix B - VMware CAIQ#1 and Appendix B – VMware CAIQ#2 for VMware's completed response. This file was uploaded separately.

Appendix C – VMware Terms and Conditions

VMware Response:

Please refer to files Appendix C for all of VMware's terms and conditions. These files were uploaded separately.

Appendix D – Resumes

VMware Response:

Please refer to the following files for resumes.

- VMware Resume – Karin Whitwood
- VMware Resume – Peter Brandano

These file were uploaded separately.

Appendix E – VMware Marketing Plan

VMware Response:

Please refer to Appendix E for VMware's Marketing Plan. This file was uploaded separately.

Appendix F – VMware Financial Solutions (VFS)

VMware Response:

Please refer to Appendix F for a copy of VMware's Payment Plan Agreement. This file was uploaded separately.

Appendix G – Confidentiality Claim Form

VMware Response:

VMware's response does not contain any information that VMware considers confidential or proprietary. We have not submitted the Claim of Business Confidentiality form.

Appendix D – Resumes

D.1 Karin Whitwood

Summary of Qualifications and Professional Experience

Accomplished Senior Contracts Administrator with 10+ years' progressive leadership experience across federal, state & local government contracting and commercial contracting. Dedicated to identifying, analyzing, and mitigating risk. Instrumental in improving processes, reducing redundancies, enhancing information accuracy, and developing best practices. Solid comprehension of FAR, DFARS and multiple states' procurement regulations. Proven ability to communicate and collaborate effectively with internal and external customers at all levels of an organization, including C-level executives. Experience includes providing full contract life cycle support in pre-award and post-award phases, primarily with strategic contract management requirements including direct awards, indirect, IDIQ master contract vehicles. Supporting business development and capture management teams in pursuit of new business and analyzing RFx, develop and review proposals, contract awards and modifications. Preparation and negotiation of contract agreements (NDA, TA, Subcontracts, prime contracts T&Cs). Administration of prime contract management plans, reporting requirements and submissions, monitor contract performance for federal, state and local government contracts including GSA schedules, GWACs, state MASs. including risk mitigation in contract pre- and post-award activities.

EDUCATION, CERTIFICATIONS, SKILLS AND TOOLS

Bachelor of Arts in Communications ~ Randolph-Macon Women's College
Applied Associates in Nursing ~ Northern Virginia Community College for Nursing
Graduate-Level Legal Studies ~ Catholic University School of Law
Graduate-Level MBA Studies ~ Marymount University MBA Program
Ongoing Professional Education ~ NCMA seminars and conferences

Active Top Secret Security Clearance (TS/SCI). Member, NCMA.

RELEVANT CORE COMPETENCIES

- Contract Administration
- RFx Analysis & Review
- Risk Analysis & Mitigation
- Project Management
- Proposal Development
- NDA/TA preparation & Negotiation
- Government Reporting Regulatory Compliance
- Contract terms negotiations
- Procedural Development
- MAS, MAC Contract Vehicles
- Client Relations Management

Proficient in: MS Office, Deltek CRM, Costpoint and various proprietary database applications

Work experience

VMware, INC., Reston, VA, Contracts Manager	2014- 2015
L-3 NATIONAL SECURITY SOLUTIONS, INC., Reston, VA, Sr. Contracts Administrator	2014- 2015
GRANT THORNTON LLP, Alexandria, VA, Contract Manager	2010–2014
BUREAU OF NATIONAL AFFAIRS / BLOOMBERG, Arlington, VA	1994–2004
Contract Administration Manager	1999-2004
Contract Renewal Pricing Manager	1998-1999
Market Research Analyst	1996–1998
Senior Information Specialist	1994-1996

D.2 Peter D. Brandano

Summary of Qualifications and Professional Experience

Senior level Data Center and Cloud Solutions Manager, Mr. Brandano brings more than 16 years of experience providing strategic & tactical planning, development, evaluation, and coordination of Cloud, Cybersecurity, IOT, Simulation & Modeling and enterprise IT infrastructure, systems, and applications. Collaborate across the corporation ensured alignment and consistency of strategies and shared resources. He reviewed/Approved major contracts for IT hardware, software and services and drive down vendor costs. Provided technical expertise in existing projects and business development efforts, and concisely convey the technical approach and strategy to all internal and external stakeholders. Managed, coached, & directed solutions architecture teams to build engineering, presentation, and selling skills

Formally, Mr. Brandano evaluated new relevant technologies, trends, policy and regulations to identify potential cost savings and value for our customers and to ensure compliance with industry standards. Audited the quality, accuracy, compliance and completeness of team and vendor/partner pricing and deliverables.

Mr. Brandano lead and managed IT portions of GDIT's Energy Savings Performance Contracting Initiatives which allows customers to turn OpEx savings into CapEx to fund IT with projected energy savings over an extended period. He envisioned, designed, architected and created GDIT's OpenStack-based Secure Private/Hybrid cloud offering & cutting-edge Cloud Brokerage offering to minimize the cost of our IT solutions.

Mr. Brandano provided hands-on technical and business leadership & direction to the design, build and operations of the USMC's $150Mil enterprise datacenter (>500 servers & VMs) including IT HW/SW integration, information assurance, staffing, contracting, etc. In spite of the contract value, this effort was comprised of 30+ resource-constrained technical initiatives, so cost efficiency and technical creativity were required. As well as helped Texas Dept. of Public Safety to deploy 50 Mil. Automobile registration records to a cloud solution.

EDUCATION, CERTIFICATIONS, SKILLS AND TOOLS

Boston College, College of Arts and Sciences
Bachelor of Arts in Computer Science
Worcester Polytechnic Institute (in progress)
Masters: Computer Science/Computer and Communications Networks
Babson Olin School of Business (All coursework completed graduates in May 2016)
MBA (Concentrations in Business Analytics & Marketing) – Beta Gamma Sigma
Amazon Partner Network Training
Amazon Technical Professional Accreditation
Amazon Business Professional Accreditation

RELEVANT CORE COMPETENCIES

- **Programming Languages**: Flash ActionScript, JavaScript, SQL, AJAX, XML, HTML, DHTML, CSS, Tango, SQL, C#, ASP.NET, C, Java, 68000 Assembly Language, Lingo, Shockwave, TCP/IP, Network programming, OpenGL, WML, WMLScript, SCORM. Course history upon request.
- **Software:** MS Office, MS Visio, MS Project, Rational ClearCase, UCINet 6, Tableau, Symantria, NodeXL,DOORS, CVS, NetBeans, Adobe Creative Suite (Flash, Dreamweaver, Photo Shop, Illustrator, Premier, etc), General Dynamics MAIT..
- **Hardware:** Video digitizing & digital editing, scanning/OCR, video camera work, CG, PC building.
  Operating Systems: Windows 95/98/NT/2000/XP; Mac OS 8.5; Unix; Linux.

Work Patents and Publications

Co-Inventor of:
(wo/2004/001542) systems and methods for providing media content

Contributing Author:

Internet & World Wide Web How To Program –	Deitel
XML How To Program -	Deitel
eBusiness & eCommerce How To Program –	Deitel
Wireless and Mobile Business How To Program –	Deitel

Work experience

VMware, INC., Reston, VA, Technical Program Manager — 2015- Present

General Dynamics Information Technology — Apr. 2009 – Nov. 2015
Chief Architect - Defense Solutions Division — Needham, Massachusetts

KoolConnect Technologies, Inc. — Sept. 2006 – Apr. 2009
Vice President of Technology — Needham, Massachusetts

General Dynamics C4 Systems — Apr. 2001 – Sept. 2006
Senior Software Engineer — Needham, Massachusetts

Deitel & Associates, Inc., — May 2000 - Apr. 2001
Director of Multimedia / Author — Sudbury, Massachusetts

PricewaterhouseCoopers LLP. — May 2000 – Sept. 2000
Intern – OSRM/TRS(Information Assurance Practice) — Boston, Massachusetts

Boston College — Sept.1998 – May 2000
EaglesEyes Undergraduate Research — Chestnut Hill, Massachusetts