Contract #: AR3084

STATE OF UTAH COOPERATIVE CONTRACT

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

   8x8, Inc.
   Name

   2125 O' Nel Drive
   Street Address

San Jose	CA	95131
City	*State*	*Zip*

   Vendor # VC226573 Commodity Code #: 920-05 Legal Status of Contractor: For-Profit Corporation

   Contact *Name:* Holly Davis *Phone Number:* 323-807-6559 *Email:* holly@govdynamix.com

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.

3. GENERAL PURPOSE OF CONTRACT: Provide Cloud Solutions under the service models awarded in Attachment B.

4. PROCUREMENT: This contract is entered into as a result of the procurement process on FY2018, Solicitation# SK18008

5. CONTRACT PERIOD: Effective Date: Friday, August 09, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

6. Administrative Fee: 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) of contract sales 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.

7. 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 Schedule
   ATTACHMENT D: Contractor's Response to Solicitation # SK18008
   ATTACHMENT E: Contractor Services Use Policy

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

9. 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 Procurement Code, Procurement Rules, and Contractor's response to solicitation #SK18008.

10. 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. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 5 above.

CONTRACTOR

DocuSigned by:
Scott Trainor
5D25D5012437488
August 13, 2019

Contractor's signature | Date

Scott Trainor VP, Commercial Operations

Type or Print Name and Title

DS
AC

anthony.ciccone@8x8.com

DIVISION OF PURCHASING

DocuSigned by:
Christopher Hughes
338E6D9423AB491
August 15, 2019

Director, Division of Purchasing | Date

Note: Sections negotiated 1, 2, 3, 5, 6, 7, 8, 10, 11, 13, 17, 19, 20, 21, 23, 26, 31, 32, 35, & 46.

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] and Attachments to the Master Agreement;
    (a.) Any conflicts between Attachment A and the other Attachments will be resolved in the order those attachments are listed in section 7 on the Contract Cover (Signature) Page.
(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, subcontractors, agents and affiliates (Contractor's, "**Affiliates**") who are providing the

[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: PaaS, IaaS, and PaaS.

services agreed to under the Master Agreement.

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 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 or reasonably suspected 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.

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, including Services, software, and any incidental tangible goods.

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 education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. PHI may also include 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 the possible or actual unauthorized access to a Purchasing Entity's Non-Public Data and Personal Data the Contractor believes could reasonably result in the use, disclosure or theft of a Purchasing Entity's Non-Public Data within the possession or control of the Contractor. A Security Incident also includes a major security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to a Purchasing Entity's Non-Public Data. A Security Incident may or may not turn into a Data Breach.

Service Level Agreement (SLA) means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure, the "**Service Levels**"), (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. For avoidance of doubt, the SLA (which shall be inclusive of termination rights for chronic service outages) shall set forth Purchasing Entity's sole and exclusive remedies with respect to any outages, downtime, or interruptions with respect to the Services or any failure by Contractor to meet such Service Levels as contained within the SLA.

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 a solicitation document or contract that describes the professional services to be undertaken by Contractor to configure, customize and perform other work or on-premises service for Purchasing Entity (the, "**Professional Services**").

Use Policy means the Use Policy provided in Attachment E, and any user of Contractor's Services under this Master Agreement and any Participating Addendum shall fulfill all of its obligations, representations, warranties, and covenants thereunder.

3. Term of the Master Agreement: Unless otherwise specified as a shorter term in a Participating Addendum, the term of the Master Agreement will run from contract execution to September 15, 2026 (the stated term herein and/or the term in any Participating Addendum the "**Term Period**").

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 (and such written approval shall not be unreasonably withheld and shall be provided to Contractor as promptly as reasonably practicable by the Lead State).

The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint.

6.1. Discount Guarantee Period: All baseline discounts as provided in Attachment C (the, "**Base Rates**") must be guaranteed for the entire term of the Master Agreement. Such Base Rates shall be available to any Participating Entity and Purchasing Entity seeking Services from Contractor under this Master Agreement. A price or rate reduction from the Base Rates will apply automatically to the Master Agreement and an amendment is not necessary. Notwithstanding the foregoing, at the sooner of (a) any term period and (b) a period of three (3) years, Contractor may, with sixty (60) days notice before the end of the applicable period designated in subclause (a) or (b), raise the pricing of the applicable Services up to the Base Rates. In addition, where a Purchasing Entity terminates a portion of the ordered Contractor Services under Section 7.1 (Termination) and/or the applicable Participating Addendum, Contractor reserves the right to increase the pricing for the applicable Services to the Base Rates.

7.1. Termination: Unless otherwise stated, this Master Agreement may be terminated by either party upon 120 days written notice prior to the effective date of the termination. Further, either party under a Participating Addendum may terminate such addendum upon 90 days written notice to the other Party, unless otherwise limited or stated in such 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 of the Parties, including any indemnification obligation, 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. Upon termination of this Master Agreement, all applicable Participating Addenda will continue according to its terms for the remainder of the applicable term period (as provided on the applicable Participating Addendum).

7.2. Validity of Orders: Where a Purchasing Entity places an Order for Services prior to the expiration of termination of this Master Agreement, which by its terms would extend beyond the expiration or termination of this Master Agreement, and Contractor has accepted such Order(s) prior to the expiration or termination of this Master Agreement, then any such Purchase Orders: (i) shall remain in effect and be governed by the terms and conditions of this Master Agreement, and (ii) shall survive expiration of this Master Agreement in accordance with the terms herein (and any additional terms and/or term length set out in a Participating Addendum) but will not be considered as an extension of the term of this Master Agreement nor a renewal thereof. No orders placed after expiration or termination of this Master Agreement shall be valid.

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, (6) (subject to applicable laws for any Purchasing Entity under a Participating Addendum) Content (as defined in the Security Exhibit to this Master Agreement) or other data submitted, transmitted, stored, or processed through Contractor's Services or otherwise received by Contractor in connection with its provision of the Services or day-to-day support or administration thereof or; (7) 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, will 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 by any party under this Master Agreement 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 sixty (60) calendar days after the institution or occurrence thereof

b. Upon the occurrence of an even under subsections 1-4 of this Section 10, the applicable Party shall issue a written notice of default to the breaching Party, identifying the nature of the default, and providing a period of 30 calendar days in which such Party shall have an opportunity to cure the default. Where the Contractor is in breach, 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 a bona fide and substantiated public safety matter or to prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages.

c. If either Party is afforded an opportunity to cure a breach of the Master Agreement (or a Purchasing Entity breach of the Master Agreement and any applicable Participating Addendum) and fails to cure the default within the period specified in the written notice of default, such Party shall be in breach of its obligations under this Master Agreement and the aggrieved Party 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, where Contractor has materially breached the Master Agreement and substantial harm is being done to another party as a direct result of such material breach, until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, the aggrieved Party 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 Party pursuant to a breach of the other Party's obligations under the applicable commercial code.

11. Changes in Contractor Representation: The Contractor shall make reasonable efforts to, where warranted, notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change where reasonably practical (i.e. when such personnel is directly involved in the implementation of Services for a Participating Entity and/or identified as a key executive employee of Contractor).. 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.

13.1 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, agents, and employees as well as any person or entity for which they may be liable, from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to property arising directly or indirectly from act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the on premises provision or implementation (pursuant to any SOW) of the Services and/or Contractor's gross negligence under the Master Agreement.

b. Contractor Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to any claims arising from the combination of the Product with any other product, system or method, unless the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor to work with the Product; or

(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function, and the basis of such Intellectual Property Claim is directed at Contractor's Services.

c. Purchasing Entity Indemnification. To the maximum extent permitted by applicable law, Purchasing Entities and any other user of Contractor's Services ordered pursuant to this Master Agreement and/or any Participating Addenda shall be responsible for the indemnification obligations contained with the Use Policy (Section VI).

d. The indemnified party shall notify the applicable Party within a reasonable time after receiving notice of an indemnifiable claim under this Section 13.1 (an, "**Indemnifiable Claim**"). Even if the indemnified party fails to provide reasonable notice, the indemnifying party shall not be relieved from its obligations unless the indemnifying party can demonstrate that it was prejudiced in defending the Indemnifiable Claim resulting in increased expenses or loss to the indemnifying party and then only to the extent of the prejudice or expenses. If the indemnifying party promptly and reasonably investigates and defends any Indemnifiable Claim, it shall have control over the defense and settlement of it. However, the indemnified party must consent in writing for any money damages or obligations for which it may be responsible. The indemnified party shall furnish, at the indemnifying party's reasonable request and expense, information and assistance necessary for such defense. If the indemnifying party fails to vigorously pursue the defense or settlement of the Indemnifiable Claim, the indemnified party may assume the defense or settlement of it and the indemnifying party shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the indemnified party in the pursuit of the Indemnifiable Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

13.2 EXCLUSIONS AND LIMITATIONS OF LIABILITY

a. Contractor's liability for any claim, loss or liability arising out of, or connected with the Services provided, and whether based upon default, or other liability such as breach of contract, warranty, negligence, misrepresentation or otherwise, shall in no case exceed direct damages in: (i) an amount equal to two (2) times the charges specified in the Purchase Order for the Services, or parts thereof forming the basis of the Purchasing Entity's claim, (said amount not to exceed a total of twelve (12) months charges payable under the applicable Purchase Order) or (ii) two million dollars ($2,000,000), whichever is greater.

b. The Purchasing Entity may retain such monies from any amount due Contractor as may be necessary to satisfy any claim for damages, costs and the like asserted against the Purchasing Entity unless Contractor at the time of the presentation of claim shall demonstrate to the Purchasing Entity's satisfaction that sufficient monies are set aside by the Contractor.

c. Notwithstanding the above, neither the Contractor nor the Purchasing Entity shall be liable for any consequential, indirect or special damages of any kind which may result directly or indirectly from such performance, including, without limitation, damages resulting from loss of use or loss of profit by the Purchasing Entity, the Contractor, or by others.

d. The foregoing limitation of liability in Section 13.2 (a) shall not apply to:

1. Contractor's liability under Section 13.1 (Indemnification);

2. Contractor's liability for its breach of its data security obligations under Exhibit 1 to this Master Agreement that results in the unauthorized use or disclosure of Content (as defined in such Exhibit 1 to this Master Agreement) (such maximum liability of Contractor or its affiliates for such breach shall in no case exceed $4,000,000); and

3. Contractor's obligation to provide certain credit monitoring services as set forth in Section 5 (Personal Data Breach Responsibilities), subsection (c), subclauses (1)-(5) of Exhibit 1 to this Master Agreement (where such limitation of liability is provided in subclause (4) of the aforementioned Section 5(c)(1-5)).

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 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.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below, with no deductible 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. 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 an occurrence form 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 shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shall have been given to Purchasing Entity and Participating Entity by the Contractor.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, 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 Purchase 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 to operate in all states); a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

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 within the United States.

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) The total amount of fees for Services under the Order; 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. Purchasing Entities shall not place any Orders 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. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. 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 the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, 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

[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.

Entity as explicitly permitted under this agreement; sales of goods (i.e. equipment and other hardware, but not to include any Contractor Services or any underlying intellectual property) to the general public as surplus property; 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: Orders under this Master Agreement are fixed-price or fixed-rate orders, not cost reimbursement contracts. All amounts billed by Contractor to the applicable Purchasing Entity ("**Billed Amounts**") shall be due within thirty (30) days of invoice date (Net 30), and shall be timely paid by Purchasing Entity by credit card, check, ACH, or wire transfer and without counter-claim, set-off, withholding, or deduction of any sort. Delinquent Billed Amounts shall, beginning on the fifteenth (15^{th}) day after which the applicable Billed Amounts are due, accrue interest at the rate of the lesser of one percent (1%) per month or the maximum rate permitted by applicable law. Except as expressly provided otherwise in the Master Agreement or applicable Participating Addendum, all payments to Contractor shall be non-refundable and non-creditable.

Purchasing Entities shall be responsible for and shall pay in accordance with this Section 21 (Payment), any applicable usage charges of the sort set forth (which shall include, for avoidance of doubt, charges for overages and international dialing) at the time of such usage at www.8x8.com/terms-and-conditions/usage.

If a Purchasing Entity believes in good faith that a Billed Amount was not actually incurred under the applicable Participating Addendum (i.e., was overbilled), then Purchasing Entity may dispute such Billed Amount by providing notice to Contractor by email to claims@8x8.com within thirty (30) days of the date of the first invoice in which the Billed Amount was invoiced, which such notice must specify the particular Billed Amount(s) in dispute and the basis of the dispute in reasonable detail. Failure to so dispute a Billed Amount within such period shall constitute a complete and irrevocable waiver of Purchasing Entity's right to dispute such Billed Amount. If Purchasing Entity disputes such Billed Amount in good faith in accordance with this Section 6.3 (Billing Disputes), then Purchasing Entity may, at its option, either (a) pay such Billed Amount expressly under protest or (b) withhold payment of such Billed Amount, in which case such Billed Amount, if (and only if) actually incurred under the Participating Addendum (i.e., not actually overbilled), shall not become due until ten (10) days after Contractor's confirmation of the same (if such due date is later than the original due date for such amount).

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 Data with its parent corporation, other affiliates, or any other third party without the Purchasing Entity's express written consent.

Contractor will ensure that, prior to being granted access to the Data, Contractor Staff who perform work under this Agreement have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

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 materially 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, including metadata.
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. The right to audit under this subsection (a) can be exercised once per calendar year by each applicable Participating Entity (and shall be undertaken at the cost of the requesting party). The foregoing limitation on number of audits shall not apply where Contractor has materially breached the Master Agreement, a Participating Addendum or any amendments or exhibits attached thereto.

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 (as governed by the terms of this Master Agreement or any Participating Addendum).

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 best efforts to restore or assist in restoring the system to operational capacity.

29. Title to Product: If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity an irrevocable and perpetual license to use the API.

30. Data Privacy: The Contractor must comply with all applicable laws related to data privacy and security, including IRS Pub 1075. 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 Contractor must document the Data Categorization in the SLA or Statement of Work.

31. Warranty: At a minimum the Contractor must warrant 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 in the United States.

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 will not interfere with a Purchasing Entity's access to and use of the Services it acquires from this Master Agreement unless as specifically set out in this Master Agreement, a Participating Addendum, or the Use Policy.

e. The Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its response to the Solicitation by the Lead State pursuant to any specifications contained within this Master Agreement, a Participating Addendum and/or any SLA.

f. The Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. The Contractor shall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at Contractor's standard professional services rates. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, at Purchasing Entity's cost, 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 Data 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 directors or executive officers 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 it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

39. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered into a multi-year agreement with JAGGAER, formerly SciQuest, whereby JAGGAER 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://calculator.naspovaluepoint.org. 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 H.

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.

43. NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review:

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor’s contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor’s website has been updated to properly reflect the contract offer as available in the participating state.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.

d. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.

e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.

f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, terminate the Master Agreement pursuant to section 6 when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. This subsection does not limit the discretionary right of either the Lead State or Contractor to terminate the Master Agreement pursuant to section 7.

g. Contractor agrees, within 30 days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-part contracts or agreements that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this master agreement. Upon request of the Lead State or NASPO ValuePoint, Contractor shall provide a copy of any such provisions.

45. NASPO ValuePoint Cloud Offerings Search Tool: In support of the Cloud Offerings Search Tool here: http://www.naspovaluepoint.org/#/contract-details/71/search Contractor shall ensure its Cloud Offerings are accurately reported and updated to the Lead State in the format/template shown in Attachment I.

46. Entire Agreement: This Master Agreement, along with any attachment, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum with a Participating Entity. 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 (unless specifically set out in this Master Agreement and any other attachments and the applicable Participating Addendum), even if use of such Services requires an affirmative "acceptance" of those Additional Terms before access is permitted.

Exhibit 1 to the Master Agreement: Software-as-a-Service

Capitalized terms used and not defined herein shall have the meanings assigned to them in the Master Agreement.

1. Data Ownership: The Purchasing Entity will own all right, title and interest in the content (including all Data therein) of all communications transmitted, received, and/or stored through any Services ("**Content**"). The Contractor shall not access Purchasing Entity Content, except (1) in connection with performing under the Master Agreement (which shall, for clarity, include providing, supporting, or enhancing (e.g., performing quality control functions) the Services; in the course of data center operations; and in response to service or technical issues), (2) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (3) at the Purchasing Entity's request or instruction, or as approved in advance in writing by Purchasing Entity, or (4) for the purpose of complying with any law, regulation, ordinance, or court or administrative order or ruling, or subpoena, civil investigation demand, or other legal process (collectively, the "**Authorized Purposes**").

Contractor shall not collect, disclose to non-Affiliate third-parties, or use user-specific Purchasing Entity Content except as reasonably necessary to perform an Authorized Purpose. No information regarding a Purchasing Entity's use of the Service may be 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. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to safeguard against unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality and integrity of Purchasing Entity Content and comply with the following conditions:

a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data in Content. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. All Purchasing Entity Content obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

c. All Personal Data in Content shall be encrypted at rest and in transit with controlled access while within 8x8's systems. All Personal Data in Content, while within 8x8's systems, shall be protected by defensive data firewalls and protected in accordance with a security program of the sort described in this Exhibit. In addition, at Purchasing Entity's formal request to the Contractor and subject to any applicable fees or charges, all Personal Data in Content within a voicemail or voice recording stored within 8x8 Virtual Office Ordered SaaS Services and/or all Personal Data in Content within a voice recording stored within 8x8 Virtual Contact Center

Services shall be encrypted at rest with controlled access while within 8x8's systems. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data in accordance with the preceding sentences within this clause (c) (subject to the conditions set forth therein). Any such stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

d. Contractor shall encrypt all Content, including Non Public Data, at rest and in transit in accordance with Section (c) of this Exhibit.

e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any Content collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: Storage of Purchasing Entity Content from communications sent or received by the user of the Ordered SaaS Services within the United States ("**U.S.-Originated Data**") at rest shall be in data centers located solely in the U.S. The Contractor shall adopt and maintain a policy (a) forbidding its personnel or contractors from storing Purchasing Entity Content outside of Contractor systems (including on personal portable devices and personal computers) and (b) requiring its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support or using a VPN and two-factor authentication. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification:

a. Incident Response: Contractor may need to communicate with outside parties regarding a security incident resulting in unauthorized accessing, use, or disclosure of Content, which may include contacting law enforcement, fielding media inquiries and seeking external expertise, defined by law or contained in the contract. Discussing such security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon, defined by law or contained in the Master Agreement.

b. Security Incident Reporting Requirements: The Contractor shall report a security incident resulting in unauthorized accessing, use, or disclosure of Content to the Purchasing Entity identified contact immediately within thirty-six (36) hours of learning that such security incident occurred.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's Content that is subject to applicable data breach notification law in the United States and actually or likely resulted in unauthorized accessing, use, or disclosure of such Content, the Contractor shall (1) within thirty-six (36) hours, notify the Purchasing Entity, unless shorter time is required by such applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. Personal Data Breach Responsibilities: This section only applies when a data breach occurs with respect to Personal Data in Content within the possession or control of the Contractor and actually or likely resulted in unauthorized accessing, use, or disclosure of such Content.

a. The Contractor, unless stipulated otherwise, shall within thirty-six (36) hours notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been such a data breach.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 36 hours or sooner, unless shorter time is required by applicable law in the United States, if it has confirmed that there is, or reasonably believes that there has been such a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a data breach resulting in unauthorized accessing, use, or disclosure of Content is a direct result of Contractor's breach of its contractual obligations under this Exhibit to encrypt such Content or of such obligations restricting the disclosure of such Content, the Contractor shall bear the costs associated with (1) its own investigation and resolution of the data breach and (2) any notifications that it chooses to make to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: If permissible, the Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's Content and shall, if permissible, withhold production of such Content pending any lawful attempt by the Purchasing Entity to obtain a court order or other legal recourse to prevent or condition such disclosure. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. 8x8 shall delete Content (including all originals and copies of such Content) no later than thirty (30) days after the earlier of Customer's deletion of the relevant Content from the relevant account or closure of such account. Contractor shall also ensure the ability of any Purchasing Entity to recover its Content from the Services at any time up to the time of termination (where applicable).

b. During any period of service suspension not based on the Purchasing Entity's breach of the Master Agreement, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's Content.

c. Intentionally left blank by the parties.

d. The purchasing entity shall be entitled to any post termination assistance generally made available with respect to the Services as outlined in the Master Agreement, this Exhibit, or any Participating Addendum, unless a unique data retrieval arrangement has been established as part of an SLA.

e. In deleting Content as required under clause (a) of this Section 7 (Termination and Suspension), Contractor shall securely dispose of such Content in all of its forms, such as disk, CD/ DVD, backup tape and paper. In the case of deletion of Content from 8x8's systems, such deletion may be achieved via overwriting of such data in accordance with industry-standard methods. Where a hard disk used by the Contractor to store such Content is decommissioned, the Contractor shall destroy such disk in accordance with National Institute of Standards and Technology (NIST)-approved methods. Certificates of such destruction following closure of the relevant account shall be provided to the Purchasing Entity upon the Purchasing Entity's request.

8. Background Checks: Upon the request of the Purchasing Entity, the Contractor shall, to the extent permissible and feasible in light of relevant legal or regulatory requirements, conduct criminal background checks of Contractor's employees to which it provides access to the Purchasing Entity's content at or around the time of such employees' onboarding and not provide such access to any such employee who has been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony. Additionally, the Contractor shall require any subcontractors to whose personnel the Contractor provides access to the Purchasing Entity's Content to conduct a background check of such personnel, to the extent permissible and feasible in light of relevant legal or regulatory requirements. The Contractor shall promote and maintain an awareness of the importance of securing its customers' information among the Contractor's employees and agents.

9. Data Centers and Verification of Security. The Contractor shall closely monitor system traffic relevant to the security of the Purchasing Entity's Content in accordance with industry standards. The Contractor's hardware and software systems used to store the Purchasing Entity's Content shall be hosted at top tier data centers that are SOC 2 Type 2 compliant. At least annually Contractor shall ensure any such hosting service provider utilized by Contractor to store such Content shall conduct a SOC 2 Type 2 audit of its information security programs and, upon request following such audit(s), Contractor shall promptly provide the findings in writing to the Purchasing Entity. In addition, upon the Purchasing Entity's request (via reasonable notice to the Contractor) and in order to verify the Contractor's security status and compliance with the security requirements of this Exhibit, the Contractor shall provide to the Purchasing Entity any of the following (as so requested): (i) an executive overview of the Contractor's security program, (ii) a copy of the Contractor's then-current FISMA attestation (or attestation or similar document of a similar data protection standard), (iii) an executive overview of veracode SAST and DAST scans showing no unresolved critical or high vulnerabilities in the Contractor systems used to store or process the Purchasing Entity's Content.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms in accordance with the audit rights set out in the Master Agreement. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall house the appropriate equipment related to the transmission of Customer Content in top tier Soc 2 Type 2 compliant data centers. 8x8 shall be obligated to provide confirmation of such SOC 2 compliance upon a Purchasing Entity's reasonable request.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice, where practicable and where Contractor provides such notice across a majority of its customer base, or otherwise shortly thereafter (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

13. Intentionally Left Blank by the Parties.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity Content to that which is reasonably necessary to perform job duties.

15. Import and Export of Data: Contractor shall make Purchasing Entity's Content available for download at Purchasing Entity's request (which shall be a functionality of Contractor's Services).

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the Contractor platform supporting the SaaS services being provided under the Master Agreement. The technical and professional activities required for establishing, managing and maintaining the environments related to such platform are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime and any other provisions contained in the SLA concerning uptime and/or downtime) and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Subject to Contractor's confidentiality obligations to any third party, Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement upon a Purchasing Entity's reasonable request, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations. Any request that would require Contractor to divulge proprietary information about its Services or other products shall not be deemed reasonable for purposes of this Section 17.

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to require that the Contractor remove from any interaction as part of any work performed at a Purchasing Entity site any Contractor representative who the Purchasing Entity reasonably believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity credibly signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the person to any aspect of the Master Agreement or future work on-site orders without the Purchasing Entity's consent.

19. Business Continuity and Disaster Recovery: The Contractor shall implement a business continuity and disaster recovery plan and, upon request from the Purchasing Entity, provide an executive overview of such plan(s) Contractor shall perform an annual disaster recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

20. Compliance with Accessibility Standards: Where required by applicable law, the Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the Participating Entity.

21. Intentionally Left Blank by the Parties.

22. Intentionally Left Blank by the Parties.

23. Subscription Terms: Contractor grants to a Purchasing Entity (subject to the Use Policy attached to the Master Agreement) a license to: (i) access and use the Service for its business purposes; (ii) for SaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

24. Broader Contractor Obligations. Purchasing Entity acknowledges that Contractor and its Affiliates are subject to various obligations under laws, regulations , administrative orders, rulings, and guidance, etc., and industry frameworks, with respect to various categories and sets of data, and agrees that the requirements of these security and data protection terms shall in all cases be subject to the Contractor's and its Affiliates' fulfillment of such obligations and compliance with the foregoing. Accordingly, in no event shall any provision of these security and data protection terms be construed to require the Contractor or its Affiliates or partners to perform any act or omission that might cause any of them to violate any such obligation.

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Software as a Service (SaaS)

1.2 Risk Categorization.*

Contractor's offered solutions offer the ability to store and secure data under the following risk categories:

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
SaaS	x	x		Public

*Contractor may add additional OEM solutions during the life of the contract.

2.1 Deployment Models.

Contractor may provide cloud based services through the following deployment methods:

- **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Attachment C - Pricing Discounts and Schedule

Contractor: 8x8, Inc.

Pricing Notes

1. % discounts are based on minimum discounts off Contractor's commercially published pricelists versus fixed pricing. Nonetheless, Orders will be fixed-price or fixed-rate and not cost reimbursable contracts. Contractor has the ability to update and refresh its respective price catalog, as long as the agreed-upon discounts are fixed.
2. Minimum guaranteed contract discounts do not preclude a Contractor and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.
3. Purchasing entities shall benefit from any promotional pricing offered by Contractor to similar customers. Promotional pricing shall not be cause for a permanent price change.
4. Contractor's price catalog include the price structures of the cloud service models, value added services (i.e., Maintenance Services, Professional Services, Etc.), and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing shall all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.
5. Contractor's discount is the discount off Contractor's commercially published pricelists versus fixed pricing. Orders, however, will be fixed-price or fixed-rate and not cost reimbursable contracts.

Cloud Service Model: Software as a Service (SaaS)

Description	Discount
SaaS Minimum Discount % (applies to all OEM's offered within this SaaS model)	5.00%
Average SaaS OEM Discount Off	**5.00%**

Additional Value Added Services

	Onsite Hourly Rate		Remote Hourly Rate	
Item Description	**NVP Price**	**Catalog Price**	**NVP Price**	**Catalog Price**
Maintenance Services	N/A	N/A	N/A	N/A
Professional Services				
Deployment Services	N/A	N/A	N/A	N/A
Integration Services)	N/A	N/A	N/A	N/A
Consulting/Advisory Services	N/A	N/A	N/A	N/A
Architectural Design Services	N/A	N/A	N/A	N/A
Statement of Work Services	N/A	N/A	N/A	N/A
Partner Services	N/A	N/A	N/A	N/A
Training Deployment Services	N/A	N/A	$ 99.00	$ 100.00
[Insert additional value added services as necessary]	N/A	N/A	N/A	N/A
[Insert additional value added services as necessary]	N/A	N/A	N/A	N/A
[Insert additional value added services as necessary]	N/A	N/A	N/A	N/A
[Insert additional value added services as necessary]	N/A	N/A	N/A	N/A

Deliverable Rates

	NVP Price	Catalog Price
N/A	N/A	N/A

8x8

Multiply the possibilities

Response to

Request for Proposal

The State of Utah

Division of Purchasing

In conjunction with:
NASPO Value Point
Utah Solicitation Number SK18008

NASPO ValuePoint Master Agreement for Cloud Solutions

Technical Response

High-powered communications and collaboration solutions that grow with your enterprise and unite teams worldwide for maximum productivity and impact.

Table of Contents

8x8 Technical Response

If applicable to an Offeror's Solution, an Offeror must provide a point by point response to each technical requirement demonstrating its technical capabilities. If a technical requirement is not applicable to an Offeror's Solution then the Offeror must explain why the technical requirement is not applicable.

If an Offeror's proposal contains more than one Solution (i.e., SaaS and PaaS) then the Offeror must provide a response for each Solution. However, Offerors do not need to submit a proposal for each Solution.

8x8's offered solution to the response of the RFP is for a SaaS delivery model.

8.1 (M)(E) TECHNICAL REQUIREMENTS

8.1.1 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 characteristics defined in NIST Special Publication 800-145.

8x8's solutions are compliant and meet the NIST requirements of the RFP as stated in the NIST Special Publication 800-145. Compliance with NIST Special Publication 800-145 was reviewed and 8x8 assures the understanding of the requirement. According to the NIST requirements as described in the Attachment C: NIST Service Models 8x8's solution is SaaS secured hosted voice and collaboration solutions through a Public Cloud deployment model.

8.1.2 As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of **Attachments C & D**.

8x8 as the Offeror in our response are willing to fully comply with the requirements of Attachments C & D of the RFP.

8.1.3 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**.

8x8's proposal adheres to the services, definitions and deployment models as identified in the Scope of Service from Attachment D. 8x8 scope of services as designated by Attachment D as voice and collaboration services.

We are a cloud-based provider that offers world-class business phone services, collaboration and virtual meetings plus enterprise ready contact center solutions—in one secure, reliable Unified Communications Platform.

8x8 cloud-based services provides the ability to store and secure one, all, or a combination of data for communications. Authorized administrators would be able to perform basic tasks such as Moves, Adds, Changes and Deletes. 8x8's Virtual Office enables end users to manage personal directory, speed dials, their voicemail account, call forwarding and conferencing from multiple platforms.

Our SaaS offering is deployed through the public cloud and we consider our solution as a "Moderate Risk Data".

8.2 (E) SUBCONTRACTORS

8.2.1 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.

8x8 operates business in a direct and indirect model by utilizing direct teams and highly qualified Affiliate (subcontractors). 8x8 may, in each case designate an 8x8 Affiliate to enter into one or more Orders or SOWs with Participating Entities, in which case, with respect to such Orders or SOWs, unless otherwise agreed in writing by the Parties.

(1) any Agreement's references to "8x8" shall include such 8x8 Affiliate (as well as 8x8) (provided that the 8x8 affiliate shall be deemed to be the service provider under such Orders or SOWs) and
(2) 8x8 shall remain fully, including jointly and severally liable under any Agreement and (b) subcontract for the performance of 8x8's obligations under any Agreement, provided that 8x8 shall remain responsible for performance of such obligations and for such subcontractors' actions or omissions in performing such obligations.

8.2.2 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.

8x8 Subtractor's (Affiliates) provide sales and services to include, but are not limited to: network assessments, installations, and Tier 1 support. Each of these partners is also responsible for providing any on-site hardware necessary for the deployment of the 8x8 solution.

All subcontractors (Affiliates) of 8x8 will be held accountable to the terms and conditions of the Master Agreement through an addendum within their 8x8 partner agreement.

8.2.3 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.

All of 8x8 authorized partners (subcontractors) are held accountable to the partnering agreements with 8x8. All subcontractors who wish to collaborate with 8x8 working with Purchasing Entities will be held accountable to all of the requirements of the Master Agreements, SLA and the Statements of Work.

8x8 remains fully, including jointly and severally liable under any Agreement which includes obligations from the performance of the subcontractor.

8.3 (E) WORKING WITH PURCHASING ENTITIES

8.3.1 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;
    - If any data breach were to occur the contract manager as stated in Section 7 of the RFP would be assisting as the liaison and support in relation to all contractual agreements between the parties adhering to the SLA. The additional parties from 8x8 who would be involved to support a data breach would be; customer support, engineering, and the 8x8 account manager.
    - In addition to the above support 8x8 in case of a data breach 8x8's head of information security and compliance would be involved. Our compliance officer has more than 20 years of information security experience in financial services, healthcare and other industry verticals at companies such as Visa and HP professional services.

- Response times;
    - Response Time Commitments. 8x8 shall use commercially reasonable efforts to respond to data breach, 24x7x365 that are reported through one of 8x8's Customer Support channels listed at http://www.8x8.com/Support.

- Processes and timelines;
    - A Data Breach would be classified as a Top Tier 8x8 Level 0 for support and would follow Service Level Agreements during and after the data breach has been resolved.

- Methods of communication and assistance; and
    - In the instance of a data breach 8x8 would notify each Customer affected by the security breach within 48hours or in accordance with applicable laws/regulations and any specific terms of the SLA with the Purchasing Entity as noted in Section 8.6.8.
    - Customer Support, assigned Purchasing Entity contact, and compliance officer would be engaged in the communications.

- Other information vital to understanding the service you provide.
    - We have provided over 250 business associate agreements (BAA) protecting our customers from any risk of HIPAA data exposure from their 8x8 implementation.
    - Have externally validated support for security regulations and standards including HIPAA, Privacy Shield, and FISMA
    - Established a Security Compliance Office led by a security leader with over 20 years of security industry experience.

8.3.2 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.

Prior approval from the 8x8 contract manager would be a requirement of any agent or partner prior to any use of marketing materials being used in conjunction of the Participating Entity or the Master Agreement. 8x8 holds any of its authorized "Affiliates" to strict rules of engagement and has the authority to cancel the agreement between 8x8 and the Affiliate at any time.

8.3.3 Offeror must describe whether its application-hosting environments support user test/staging environment that is identical to production.

8x8's application-hosting environments support a user test/staging environment that is identical to production, we refer to this service as Pilot Migration. Attaining a pilot or test of services is easy to deploy and implement. Pilot Migration for testing of the environment is provided at no cost.

We understand that there are circumstances in which a test or staging would be necessary. We stand behind our solution to provide a successful 8x8 pilot to ensure the transition to production is much easier for the participating entity.

8.3.4 Offeror must describe whether or not its computer applications and Web sites are accessible to people with disabilities and must comply with Participating Entity accessibility policies and the Americans with Disability Act, as applicable.

8x8 provides a secure hosted voice and collaboration service and provides web-based administrative and user interfaces for Purchasing Entities. Our policies comply many of the requirements, as stated below, of the Americans with Disabilities Act (ADA) per section 508, sub section; 1194.21 technology standards. We are always actively improving our standards to meet ADA requirements to best support all needs of the all users within the community in need of collaboration and voice communications.

- The contrast and colors of our web pages are designed to be readable by persons with color blindness.
- Many of the VCC agent user interface features have short cut keys, however not all features are accessible using short cut keys.
- Audible screen readers- An agent should be able to visually recognize the large functional blocks of the application to be able to navigate through processing an interaction.
- Application characteristics support visually impaired agents at a number of 8x8 sites handling voice interactions.

8x8's supported Polycom VVX phones will provide TDD/TTY capabilities. 8x8's service does not impede (i.e.: contribute to or detract from) that device working and providing these particular capabilities. 8x8 is agnostic as to what devices like this are attached to a phone. 8x8 sends / receives audio to the phone, and the phone sends/receives audio to the hearing-impaired devices.

8.3.5 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 a minimum.

8X8 applications and content are delivered through current released versions of the following browser platforms: Internet Explorer, Firefox, Chrome and Safari.

8.3.6 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.

8x8 agrees to work in conjunction with the Purchasing Entity through meetings to determine if there is any sensitive or personal information which would be used by 8x8 and is subject to any law, rule or regulation providing for the specific compliance obligations.

We will include this requirement on our internal process checklist for execution of SLAs with Purchasing Entities.

8.3.7 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.

At 8x8 we ensure our customers have a well-planned project schedule for fast and efficient migration to our solution.

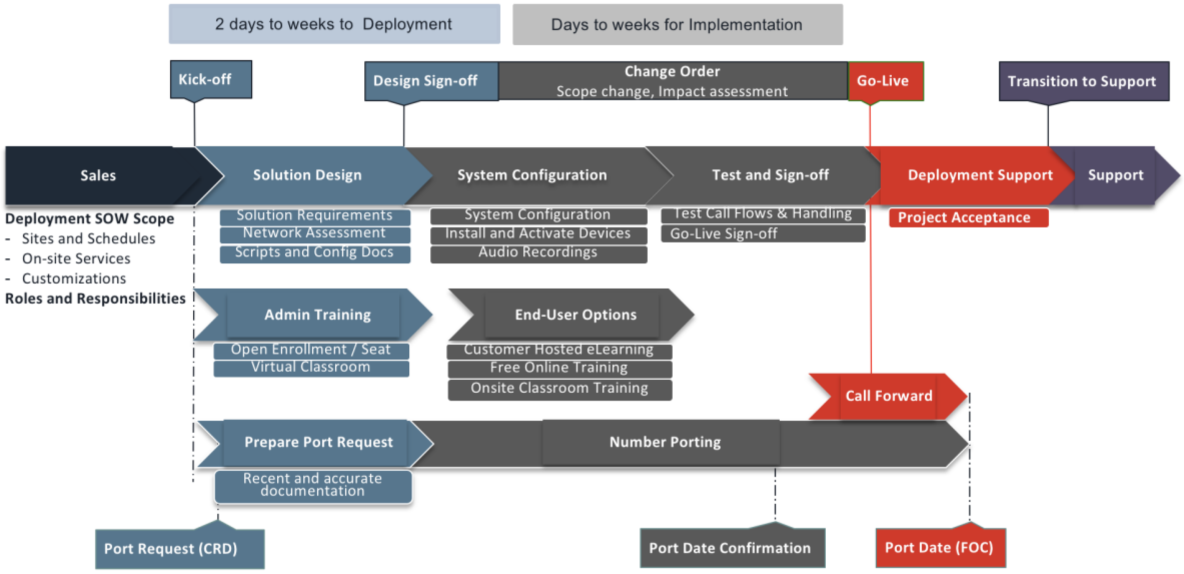
Project timelines vary due to the size and scope of the solution and if the Purchasing Entity is migrating from a traditional PBX. This may which may require additional infrastructure upgrades.

Factors to consider which may impact the length in timing for project schedule:

- Complexity of the Purchasing Entities environment.
- Is the solution unified voice communications or is contact center being implemented as well?
- Size and scale of the deployment such as multiple locations.
- Number porting dependent upon a third party to release the numbers to 8x8.

Here is an example of a traditional project schedule to time to implement the solution.

Example of Timeline



8.3.8 The State of Utah expects Offeror to update the services periodically as technology changes. Offer must describe:

- How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.

  8x8 agrees to comply with the requirements by responding to RFP if required and necessary for updating the services for technology changes per section 2.12 and 8.3.8 of this RFP.

- How Offeror will maintain discounts at the levels set forth in the contract.

  8x8 agrees to maintain the discount levels set forth per contract and with mutual parties agreement. Discount levels may be different for new service line additions added to the contract however pricing discounts will not change for services falling into the same service category.

- How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.

  8x8 agrees to report to the Purchasing Entities as needed regarding changes in technology and provide recommendations for service updates.

- How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.

  8x8 does not predict that there would be negative impact due to a service change because of the nature of the solution being offered to this RFP is not at a high risk of negative impacts. However, 8x8 will assure Purchasing Entities we will work closely with the Purchasing Entity to provide transition support through the 8x8 Implementations Support Team and will discuss all possible negative impacting concerns due to a service change.

8.4 (E) CUSTOMER SERVICE

8.4.1 Offeror must describe how it will ensure excellent customer service is provided to Purchasing Entities. Include:

- Quality assurance measures;

Minimizing the risk of downtime—and ensuring business continuity—are key concerns for businesses with global or critical operations. With redundant data centers located thousands of miles apart, 8x8 is known for providing highly reliable hosted communications.

8x8's cloud-based SaaS business communications solutions are delivered from mirrored, top-tier, secure, fully redundant, and geographically diverse state-of-the-art SSAE 16-audite data centers. Overall, 8x8 achieved an average reliability of "four nines," or 99.997 percent uptime.

- Escalation plan for addressing problems and/or complaints; and

Support has a certification process when contacting the service hotline either by phone, email, chat where we provide Tier level 1 and 2 support directly to a customer via authorized partner or direct to 8x8. There is always help 24/7 on the web or by phone if you need help, training or need to add new services.

Within the 8x8 Account Manager the Purchasing Entity would have the ability to escalate issues with expected response time as state below:

Severity	Definition	Response Objective	Restore Objective
0	Unplanned Downtime due to Complete System Failure.	< 1 hour	8x8 will work 24 hours a day 7 days a week to restore service
1	Inoperable Business Function.	< 1 hour	8x8 will work 24 hours a day 7 days a week to restore service
2	Business Function Limitation	< 1 business day	8x8 will work during normal business hours to address issue
3-4	Limited Occurrence Customer Issue or Minor System Issue	< 2 business days	8x8 will use commercially reasonable efforts to address issue

- Service Level Agreement (SLA).

It is 8x8's goal to have 8x8 Virtual Office and Virtual Contact Center Services available to Customers twenty-four hours a day, seven days a week, 52 weeks a year, with the exception of Planned Downtime with respect to such SaaS Services, and 8x8 will endeavor to achieve at least 99.99% average annual uptime (excluding Planned Downtime) for such SaaS Services ordered under the Agreement, measured across its customer base for each such SaaS Services. 8x8's records and data shall be the basis for all service availability calculations and determinations.

In the event that Customer experiences a Level 1 or 0 Unplanned Service Interruption in any calendar month, subject to the conditions set forth in this Section 6 (Service Availability Remedies), Customer shall be eligible to receive from 8x8 a service credit.

8.4.2 Offeror must describe its ability to comply with the following customer service requirements:

a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.
8x8 will provide a lead representative for each entity and ensure the contact representative information is always current.

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.
8x8 provides 24/7 customer care for all time zones in which they can be reached via email or phone any day of the week.

c. Customer Service Representative will respond to inquiries within one business day.
8x8 agrees to provide a one business day turn around for all inquiries through our customer care which is 24/7.

d. You must provide design services for the applicable categories.
8x8 will provide design services as necessary with applicable categories.

e. You must provide Installation Services for the applicable categories.
8x8 provides installation services through our value-added authorized partners.

8.5 (E) SECURITY OF INFORMATION

8.5.1 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.

8x8 is fully compliant with the U.S. Federal Communication Commission's FCC Customer Proprietary Network Information (CPNI) regulations for protecting customers proprietary network information for holding and protecting data.

8x8's comprehensive security standards comply with the rigorous U.S. Federal Information Security Management Act (FISMA). Plus, as an option, 8x8 can offer secure solutions for private multiprotocol Label Switching (MPLS) connection solutions which are completely independent of the Public Internet.

In addition, 8x8 is fully HIPAA compliant and offers HIPPAA/HITECH compliant solutions. 8x8 has also gone through the rigor of ensuring that you can rest assured that our solutions meet the US Safe Harbor data privacy standards for all EU/EEA member states.

In addition to an encrypted chip in the 8x8 phones that provides endpoint phone verification, each SIP process is interrogated to guard against a "man in the middle" and other attacks. The voice media going over the 8x8 system lines is protected via Secure SIP over TLS and Secure Real Time Transport Protocol. Beyond this, the 8x8 systems are protected via some of the most advanced Intrusion Protection and Detection Systems available today, including 137 patented tools and utilities, a 24/7 NOC/SOC, and an award-winning Hadoop-based anomaly detection system. The 8x8 phone system is also protected against hostile state government and other attacks by two, back to back Distributed Denial of Service (DDOS) prevention and mitigation systems by Akamai (with over 200.000 servers in over 1,000 locations, and Verisign.)

Should we need to dispose of data following completion of any contract services 8x8 abides by HIPAA data exposure regulations in management of data for customer migration. 8x8 follows rules of data disposal outline by FISMA/NIST 800-53 compliance includes 2,500 areas we must maintain compliance with resulting in our having 49 Policies and Procedures and Standards, 141 Auditory IT controls, and more.

8.5.2 Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.

8x8 certifies the 8x8 Data will comply with all applicable laws related to data privacy and security, which will be defined in the relevant participating addendum or SLA.

8.5.3 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.

8x8 certifies the 8x8 Data will not access a Purchasing Entity's user accounts and/or data except in response to service or technical issues, data center operations as required by the terms of the master agreement, the applicable participating addendum, or the applicable Service Level Agreement.

8.6 (E) PRIVACY AND SECURITY

8.6.1 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.

At 8x8 we base our security policies upon NIST and FISMA guidelines specifically in concern to this requirement NIST 800-145 and 800-53. FISMA/NIST 800-53 compliance includes 2,500 areas we must maintain compliance with resulting in our having 49 Policies and Procedures and Standards, 141 Auditory IT controls, and more.

8.6.2 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.

8x8 holds the following government certifications which specifically apply to our proposal; HIPPAA, FedRAMP, FIPS-2, FISMA, NIST 800-53, Privacy Shield, OWASP, ISOQAR, CYBER Credentials.

8.6.3 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.

At 8x8, we own and manage our own software and hardware. We only contract only with highly secure top tier data centers. We place additional contractual requirements on these data centers to not only meet SSAE 16 SOC I and SOC II but also our minimum-security standards of administrative, technical and physical safeguard standards to and maintain the confidentiality, integrity and availability of these systems. For high availability all of our systems have no single points of failure and, for instance, in the U.S. we can fail over core call flow over from West to East coast data centers in 30 seconds.

8.6.4 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).

In order for 8x8, Inc. to be accepted and granted an authority to operate with various sensitive strategic entities defense contractors, Atomic Power, etc. here in the U.S. and in other countries, among other things internationally required that we were certified as fully FISMA/NIST 800-53 compliant. This is a superset of FedRAMP and NIST 800-53, our validations are expert opinions and do not expire.

FISMA/NIST 800-53 compliance includes 2,500 areas we must maintain compliance with resulting in our having 49 Policies and Procedures and Standards, 141 Auditory IT controls, and more. Our FISMA attestations came as a result of more than two years work with both IBM and a Wash. D.C. consulting firm recommended by the General on our board who sent in former presidential cyber advisor and now NATO cyber advisor – Curtis Levinson. We currently work with many secure "3 letter" U.S. agencies and defense contractors. By design, FISMA is a significant superset of SOC II Type II and other compliance standards. "FISMA/NIST 800-53" is thought by many to be the most thorough, intensive form of compliance worldwide and can only be achieved in private industry via a corporate GRC culture Governed from the top with sanctions, monitoring, and continuous training.

8.6.5 Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp High, FedRamp Moderate, etc.), and certifications relating to data security, integrity, and other controls.

8x8 complies with the Federal Information Security Management Act (FISMA) and the Federal Information Processing Standard-2 (FIPS-2). 8x8 not only meets these standards but has engineered its Virtual Office and Virtual Contact Center services to assist 8x8 customers with achieving their own compliance requirements.

In order for 8x8, Inc. to be accepted and granted an authority to operate with various sensitive strategic entities defense contractors, Atomic Power, etc. here in the U.S. and in other countries, among other things internationally required that we were certified as fully FISMA/NIST 800-53 compliant. This is a superset of FedRAMP and NIST 800-53, our validations are expert opinions and do not expire.

8.6.6 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.

8x8 is ISO 27001- and ISO 9001-certified. ISO/IEC 27001 is an internationally recognized best practice framework for an information security management system. ISO 9001 sets out the criteria for a quality management system.

8.6.7 Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

Our Virtual Office and Virtual Contact Center services allow various levels of access to restrict visibility according to the license assignment from the administrator. The administrator can grant full or limited privileges.

With 8x8, you get an easy-to-use administration portal, called the 8x8 Account Manager, for setting up and configuring your phone system, setting up extensions, Auto Attendant, and Ring Groups and more.

Online Access for Extension Users (end users) within the 8x8 Virtual Office extension users can use the Virtual Office desktop app to manage and use their extensions online. They can make calls, chat with other users, set up their call forwarding rules, see their call history, and review and manage their voicemails.

User Profiles	Visibility
End User	Limited data visibility and restricted by administrator
System Administrator	Full access and visibility to all data

8.6.8 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.

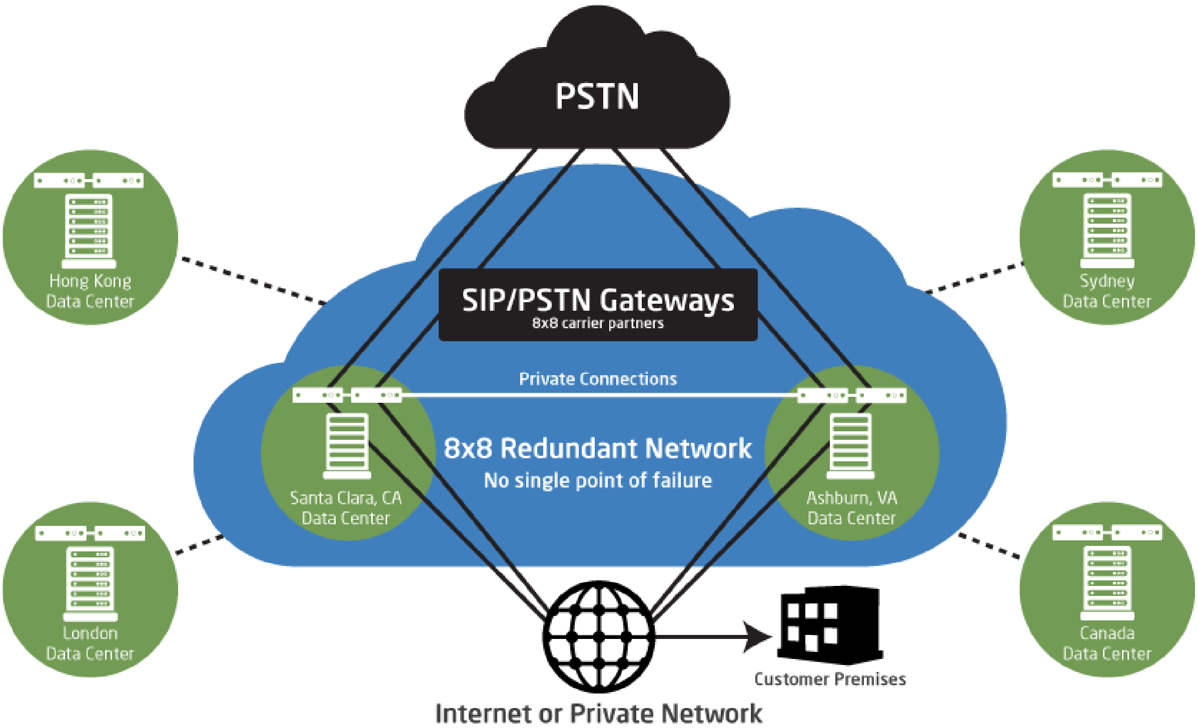
We practice secure coding with Veracode SAST and Greenlight for DevSecOPs. Our various IT groups rotate between Qualys, Tenable Nessus Pro, and Veracode DAST and SAST scans throughout our systems on a continuous basis. We bring in one of the major worldwide Pen Testing firms to Ethically Hack our systems prior to major releases. We remediate Critical and High findings right away, remediate Mediums within weeks and stay current with major vendor patches.

8.6.9 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.

8x8 communications are designed with built-in redundancy and no single point of failure. Our highly secure, top-tier data centers are located in geographically dispersed sites across the globe. These data centers are SSAE 16 audited and provide automatic and transparent failover to prevent disruptions in service. These security controls both physical and virtual ZOCA to isolate hosted servers.

8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).

8x8's cloud-based SaaS business communications solutions are delivered from mirrored, top-tier, secure, fully redundant, and geographically diverse state-of-the-art SSAE 16-audited data centers. Overall, 8x8 achieved an average reliability of "four nines," or 99.997 percent uptime in 2017.



8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

8x8 is fully compliant with the U.S. Federal Communication Commission's (FCC) Customer Proprietary Network Information (CPNI) regulations for protecting customers proprietary network information. All employees of 8x8 go through a rigorous background check prior to employment.

8x8's comprehensive security standards comply with the rigorous U.S. Federal Information Security Management Act (FISMA). Plus, as an option, 8x8 can offer secure solutions for private multiprotocol Label Switching (MPLS) connection solutions which are completely independent of the Public Internet. These requirements of the internal teams managing the data must follow these regulations/audits: plan for security, ensure that appropriate officials are assigned security responsibility, periodically review the security controls in their systems, authorize system processing prior to operations, and periodically thereafter.

In addition, 8x8 is fully HIPAA compliant and offers HIPAA/HITECH compliant solutions. 8x8 has also gone through the rigor of ensuring that you can rest assured that our solutions meet the US Safe Harbor data privacy standards for all EU/EEA member states.

8x8 is third-party certified as being a HIPAA-compliant business associate and is one of the only major cloud communications providers that openly offers business associate agreements (BAAs) to help customers comply with HIPAA requirements. 8x8 services can be configured to be HIPAA-compliant and can be set up with administrative controls and restrictions to protect stored faxes, recordings and voicemails.

8.6.12 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.

8x8 maintains FISMA/NIST 800-53 compliance. This includes 2,500 areas we must maintain compliance with resulting in our having 49 Policies and Procedures and Standards, 141 Auditory IT controls, and more. Our FISMA attestations came as a result of more than two years work with both IBM and from a Wash. D.C. consulting firm recommended by the General on our board who sent in former presidential cyber advisor and now NATO cyber advisor – Curtis Levinson. We currently work with many secure "3 letter" U.S. agencies and defense contractors. By design, FISMA is a significant superset of SOC II Type II and other compliance standards. "FISMA/NIST 800-53" is thought by many to be the most thorough, intensive form of compliance WW and can only be achieved in private industry via a corporate GRC culture Governed from the top with sanctions, monitoring, and continuous training.

8.6.13 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.

8x8 complies with all applicable laws in safeguarding client data. 8x8 has a documented response process with policies and procedures outlined to address privacy incidents, unauthorized disclosure, access or breach of client information. Should such a breach happen 8x8 would initiate our mitigation plan immediately and notify all parties effected to include the State and Cardholders associated with such data breach.

8.7 (E) MIGRATION AND REDEPLOYMENT PLAN

8.7.1 Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning 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.

When a Customer notifies 8x8 of its intention to terminate support services migrate to another provider, depending on the level of support required, 8x8 will work with the Customer and the new provider to assist with a smooth transition. 8x8 can provide the

Customer a reasonable transition period to allow its users an orderly changeover. During this transition, both parties remain bound by the terms of the service agreement, including any data security provisions.

8.7.2 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.

A customer data transfer process does not typically apply to a hosted VoIP services, such as 8x8 offers, and is not generally holding or storing customer data as such. If there is customer data to be returned, 8x8 will work with the customer to provide data delivery according to security provisions per the service agreement.

8.8 (E) SERVICE OR DATA RECOVERY

8.8.1 Describe how you would respond to the following situations; include any contingency plan or policy.

a. Extended downtime.
End to End Service Availability Commitment: 8x8 will use commercially reasonable efforts to provide Customers with an average annual "End to End" SaaS Services availability (excluding Planned Downtime) that is equal to or greater than 99.99%. 8x8's records and data shall be the basis for all service availability calculations and determinations. End to End Services availability extends the Service Availability Commitment to include Unplanned Service Interruptions caused by any failure by a Customer to access Services via an 8x8 provided IP phone (or, for 8x8's Virtual Contact Center based Services only, the 8x8 provided softphone) caused by issues associated with Customer's internet service providers or third-party telecommunications provider.

b. Suffers an unrecoverable loss of data.
8x8 solution is deployed over redundant datacenters with active- active configuration to prevent system failure. For high availability all of our systems have no single points of failure and, for instance, in the U.S. we can fail over core call flow over from West to East coast data centers in 30 seconds.

c. Offeror experiences a system failure.
Unplanned Downtime due to Complete System Failure: Level 0 issues result in complete system failure, due to the servers or network on which the SaaS Services are accessed not being available for a continuous period lasting greater than ten (10) minutes in length, but excluding the following: (i) any failure by Customer to access SaaS Services caused by any failure, interruption, outage or other factor outside of 8x8's direct control, including without limitation, issues associated with Customer's (a) computers, (b) local area networks, (c) except with respect to the End to End Services Availability Commitment, internet service providers, and any internet connectivity not under 8x8's direct control, (d) any Force Majeure event or (e) any event resulting from any actions or inactions of Customer, Customer's agents or any third parties, (ii) unavailability that is caused by any equipment that is not within the direct control of 8x8, or, except with respect to the End to End

Services Availability Commitment, third party telecommunications providers; (iii) unauthorized use of, or modifications to hardware or software, and (iv) Planned Downtime.

d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.
8x8 is able to recover and restore services and access to data within 4 business hours.

Response Time Commitments. 8x8 shall use commercially reasonable efforts to respond to Unplanned Service Interruptions, 24x7x365 that are reported through one of 8x8's Customer Support channels listed at http://www.8x8.com/Support.

e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

8x8 RPO and RTO objectives are listed below:

Severity	Definition	Response Objective	Restore Objective
0	Unplanned Downtime due to Complete System Failure.	< 1 hour	8x8 will work 24 hours a day 7 days a week to restore service
1	Inoperable Business Function.	< 1 hour	8x8 will work 24 hours a day 7 days a week to restore service
2	Business Function Limitation	< 1 business day	8x8 will work during normal business hours to address issue
3-4	Limited Occurrence Customer Issue or Minor System Issue	< 2 business days	8x8 will use commercially reasonable efforts to address issue

8.8.2 Describe your methodologies for the following backup and restore services:

a. Method of data backups
At the heart of AVTA is a multiplatform architecture that takes advantage of redundant servers, databases, and storage resources.

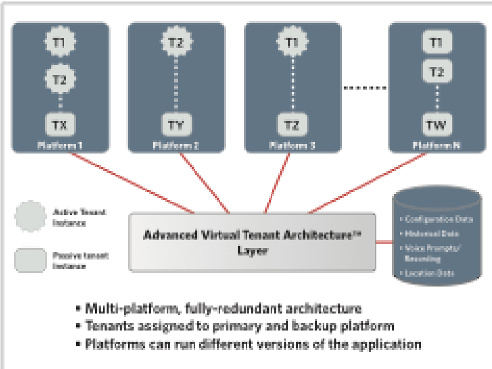
b. Method of server image backups
Servers are shared among all tenants assigned to a platform and a single platform supports hundreds of tenants. Tenants are assigned to a primary and backup platform.

c. Digital location of backup storage (secondary storage, tape, etc.)
8x8 has multiple locations of our U.S. data centers for redundancy these centers are located Santa Clara, California and Ashburn, Virginia.

d. Alternate data center strategies for primary data centers within the continental United States.
For high availability all of our systems have no single points of failure and, for instance, in the U.S. we can fail over core call flow over from West to East coast data centers in 30 seconds.

8x8 has developed its patent pending Advanced Virtual Tenant Architecture AVTA providing:

- High Availability—Best-in-class uptime at economical price points
- Virtually No Downtime for Maintenance—Most planned maintenance can be performed with no impact to customer call ow
- Minimum Upgrade Risk—Customers can upgrade to a new release of software, knowing that we can roll back at any time with no loss of data or configuration



8.9 (E) DATA PROTECTION

8.9.1 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.

8x8 has in place Data-in-motion encryption with SIP over TLS and SRTP are also available from 8x8, which enables full end-to-end encryption of both voice signaling and media streams to and through the 8x8 cloud. This capability thwarts eavesdropping attempts on your conversations or "man-in-the-middle" attacks on the IP data traversing the 8x8 cloud.

In addition, 8x8 is FISMA and FIPS – 2 certified to provide certification of high levels of encryption securities.

8.9.2 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.

8x8 would be willing to sign relevant and applicable Business Associate Agreement as necessary to protect data with a Purchasing Entity.

8.9.3 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.

8x8 commits that it will only use data for the purposes defined in the Master Agreement, participating addendums, or related service level agreements. 8x8 will not sell, participate in data mining or otherwise distribute the government data or government related data.

8.10 (E) SERVICE LEVEL AGREEMENTS

8.10.1 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.

8x8 believes our sample Service Level Agreement exceeds industry standards which are very beneficial to the purchasing entity. 8x8 would be open to negotiate if necessary.

8.10.2 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.

Per section 5.3.4 of the RFP requirements 8x8 has submitted a copy of the sample Service Level Agreement. This document defines the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

8.11 (E) DATA DISPOSAL

Specify your data disposal procedures and policies and destruction confirmation process.

8x8 is certified through multiple data security platforms one of which is NIST regulations which require proper handling of data disposal as stated below. 8x8 follows these regulations where applicable as our data exposure is low to medium risk.

- Using learning software or hardware products to overwrite storage space on the media with non-sensitive data.
- Purging magnetic media through degaussing, exposure to a strong magnetic field to disrupt the magnetically encoded information.
- Destroying the media through a variety of methods ranging from shredding to melting and incineration.

8.12 (E) PERFORMANCE MEASURES AND REPORTING

8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

8x8 offers a 99.99% Service Level Agreement, SLA for end-to-end services availability and delivered a class leading 99.9999% core system availability. This SLA also includes a MoS equivalent score call quality commitment, and response and restoration objective commitments for incidents affecting service availability and/or function.

8.12.2 Provide your standard uptime service and related Service Level Agreement (SLA) criteria.

It is 8x8's goal to have 8x8 Virtual Office and Virtual Contact Center Services available to Customers twenty-four hours a day, seven days a week, 52 weeks a year, with the exception of Planned Downtime with respect to such SaaS Services, and 8x8 will endeavor to achieve at least 99.99% average annual uptime (excluding Planned Downtime) for such SaaS Services ordered under the Agreement, measured across its customer base for each such SaaS Services. 8x8's records and data shall be the basis for all service availability calculations and determinations.

8.12.3 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.

We offer multiple points of contact for support:

- Submit a support case 24 hours a day through the 8x8 Support Knowledge Base
- Chat online
- Reach us by phone: 1-888-898-8733
- Contact the assigned 8x8 representative
- Contact the contract manager

Response Time Commitments: 8x8 shall use commercially reasonable efforts to respond to Unplanned Service Interruptions, 24x7x365 that are reported through one of 8x8's Customer Support channels listed at http://www.8x8.com/Support using the guidelines below:

Severity	Definition	Response Objective	Restore Objective
0	Unplanned Downtime due to Complete System Failure.	< 1 hour	8x8 will work 24 hours a day 7 days a week to restore service
1	Inoperable Business Function.	< 1 hour	8x8 will work 24 hours a day 7 days a week to restore service
2	Business Function Limitation	< 1 business day	8x8 will work during normal business hours to address issue
3-4	Limited Occurrence Customer Issue or Minor System Issue	< 2 business days	8x8 will use commercially reasonable efforts to address issue

8.12.4 Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.

Unplanned Service Interruption: In the event that Customer experiences a Level 1 or 0 Unplanned Service Interruption in any calendar month, subject to the conditions set forth in this Section 6 (Service Availability Remedies), Customer shall be eligible to receive from 8x8 a service credit ("Service Credit") in accordance with the following schedule:

Severity	Incidents of Actual Service Interruption or Total Aggregate Time of Service Interruption	Service Credit Equals Percent of Service Fees During Month of Unplanned Service Interruption
0	3 incidents or 3 hours	10%
0	5+ incidents or 6 hours	15%
1	3 incidents or 4 hours	5%
1	5+ incidents or 8 hours	7%

The 8x8 SLA provides service credits equaling a percentage of service fees owed by the customer during the month of the incident in question. The amount of such percentage varies depending on the severity level of the incident, the number of incidents and the amount of service interruption caused by the incident. The SLA also provides the customer with the right to terminate the service agreement for chronic unavailability.

Termination Option for Chronic Problems: In the event Customer experiences three (3) Level 0 Unplanned Service Interruptions in any single calendar month for two (2) consecutive calendar months, 8x8 will be considered to have materially breached the Agreement for purposes of Customer's right thereunder to terminate such Agreement for 8x8's material breach thereof, provided that (a) no 8x8 "cure" right shall apply with respect to such Customer termination right and (b) Customer must exercise such termination right within five (5) days following the end of the month during which such termination right arose.

8.12.5 Describe the firm's procedures and schedules for any planned downtime.

8x8 uses the following SLA's for Planned Downtime:

Planned Downtime. Planned downtime occurs when Customer has no access to the SaaS Services due to scheduled maintenance, application upgrades and similar work performed by 8x8 or 8x8's data center host ("Planned Downtime").

Scheduling of Planned Downtime. 8x8 will use commercially reasonable efforts to schedule Planned Downtime at a time and to conduct the maintenance in a manner reasonably expected to minimize the extent of the disruption on average to each affected customer.

Notice for Planned Downtime. 8x8 will use commercially reasonable efforts to provide: at least twenty-four (24) hours' prior notice of Planned Downtime that in anticipated not to exceed one (1) hour; and at least seventy-two (72) hours' prior notice of all other Planned Downtime.

8.12.6 Describe the consequences/SLA remedies if disaster recovery metrics are not met.

Termination Option for Chronic Problems. In the event Customer experiences three (3) Level 0 Unplanned Service Interruptions in any single calendar month for two (2) consecutive calendar months, 8x8 will be considered to have materially breached the Agreement for purposes of Customer's right thereunder to terminate such Agreement for 8x8's material breach thereof, provided that (a) no 8x8 "cure" right shall apply with respect to such Customer termination right and (b) Customer must exercise such termination right within five (5) days following the end of the month during which such termination right arose

8.12.7 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.

8x8 provides performance reports in real-time available robust suite of web-based tools that provide enterprise-level analytics that can be used to make highly informed business decisions. This suite of services delivers easy to use, customizable and rapid insights into the historical and real-time information associated with all extensions and devices in an organization's Virtual Office System.

Essentials

Comprehensive set of unique dashboards and reporting options for all extensions in an organization's 8x8 cloud PBX.

- Extension Summary
- Call Detail Records
- Active Calls
- Unreturned Calls
- Calls by DID

Supervisor

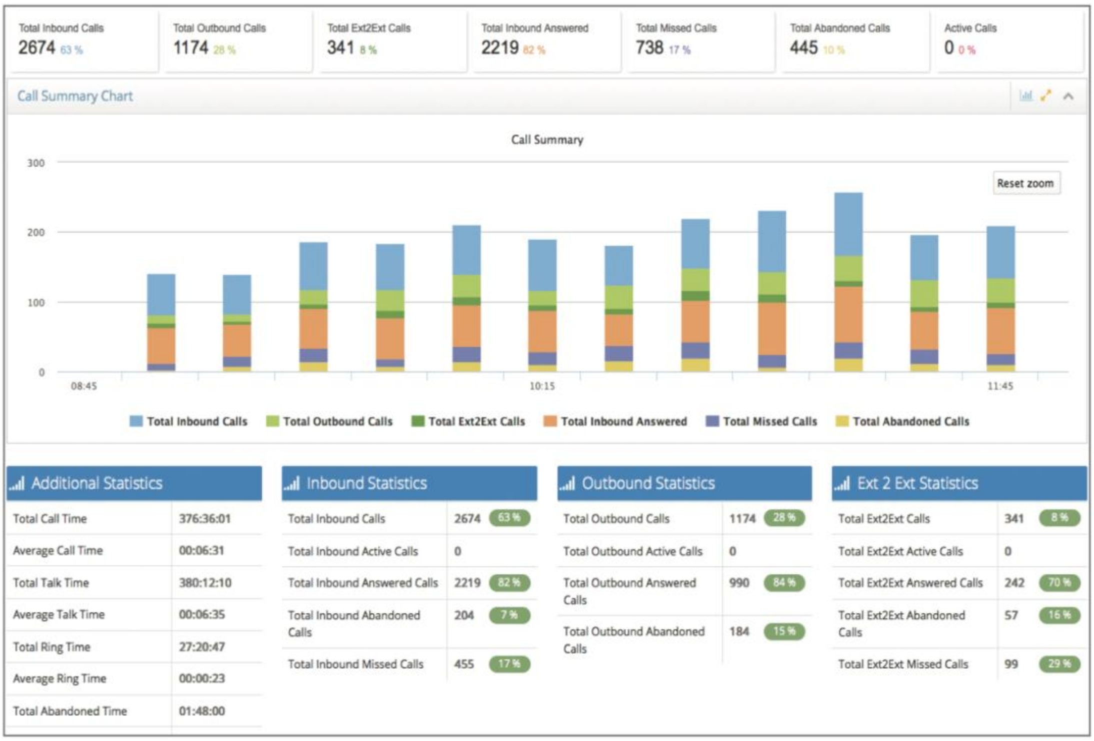
A real-time view of all call activity for selected call queues or ring groups within the 8x8 cloud PBX. Get comprehensive call center-like reporting in a single dashboard view, available on any device.

- Agent performance
- Queue status and performance

Service Quality

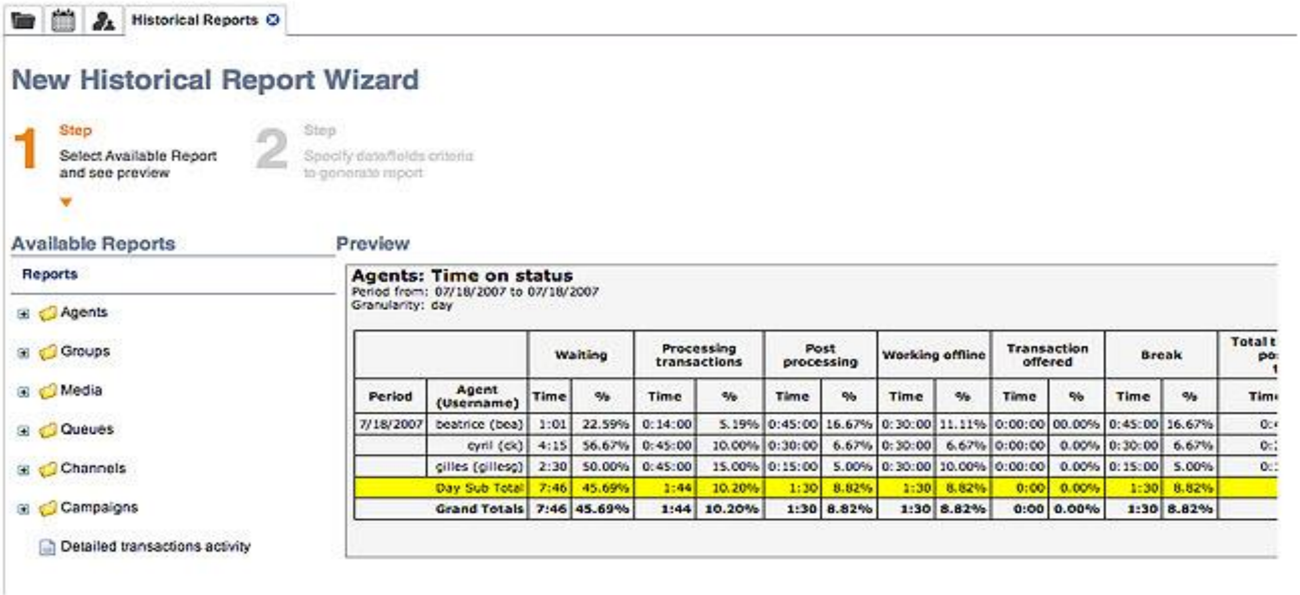
Real-time information about three important aspects of your 8x8 hosted PBX service:

- Status of all endpoint devices
- Individual call and MOS score detail
- Extension summary graphing



We provide additional Reporting through our Contact Center Application:

- Give call center managers the information they need to make smart business decisions.
- Access reports online, wherever you are—or export the data to Excel to really dig in and manage the details.
- Customize reports to show only the data you need.
- View reports by agent, agent groups, queues, date range and channel type.
- Lower costs by understanding what is working and what can be improved.
- Spot trends fast for quicker response.
- Improve the customer experience and boost customer satisfaction.



		Waiting		Processing transactions		Post processing		Working offline		Transaction offered		Break		Total t po
Period	Agent (Username)	Time	%	Time	%	Time	%	Time	%	Time	%	Time	%	Tim
7/18/2007	beatrice (bea)	1:01	22.59%	0:14:00	5.19%	0:45:00	16.67%	0:30:00	11.11%	0:00:00	00.00%	0:45:00	16.67%	0:
	cyril (ck)	4:15	56.67%	0:45:00	10.00%	0:30:00	6.67%	0:30:00	6.67%	0:00:00	0.00%	0:30:00	6.67%	0:
	gilles (gillesg)	2:30	50.00%	0:45:00	15.00%	0:15:00	5.00%	0:30:00	10.00%	0:00:00	0.00%	0:15:00	5.00%	0:
	Day Sub Total	7:46	45.69%	1:44	10.20%	1:30	8.82%	1:30	8.82%	0:00	0.00%	1:30	8.82%	
	Grand Totals	7:46	45.69%	1:44	10.20%	1:30	8.82%	1:30	8.82%	0:00	0.00%	1:30	8.82%	

8.12.8 Ability to print historical, statistical, and usage reports locally.

8x8 Virtual Office delivers an unmatched suite of analytics tools that give you enterprise-level business intelligence about your communications. Virtual Office captures finely detailed data on all call activity associated with your 8x8 cloud-based PBX—and presents it to you in easy-to-use views and reports, allowing you to take quick, decisive action. Within the Virtual Office you can print historical, statistical and usage reports from multiple platforms locally and real-time.

8.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365.

8x8 does offer on-demand deployment for current customers to add users and services to their existing account. If a Purchasing Entity is requesting to establish a new account they will need to attain a quote through the hotline 1-866-835-2979 or online https://www.8x8.com/resources/tools/request-a-quote.

With 8x8, all your communication capabilities are simple to manage and fast to deploy. Once the Purchasing Entities account is established they will have full control over their system, everywhere. Make changes, connect dispersed locations and empower employees to customize their service themselves—all without IT assistance.

8.12.10 Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

8x8's scalability up and down is available at the administrative user level 24/265.

The 24/365 scalability includes the ability to configure settings, edit extensions, add/remove services and grant privileges to other users in your system, add a user per license use agreement, upgrade or downgrade to scale users as needed. This would include the ability to access analytics and report.

8.13 (E) CLOUD SECURITY ALLIANCE

Describe and provide your level of disclosure with CSA Star Registry for each Solution offered.

8x8 has completed the CSA Star self-assessment and registry in compliance with the SaaS solution.

a. Completion of a CSA STAR Self-Assessment. (3 points)
   8x8 has completed the CSA Star Self-Assessment and attached as Exhibit 1 to Attachment B.

b. Completion of Exhibits 1 **and** 2 to Attachment B. (3 points)
   8x8 has provided Exhibit 1 to Attachment B per section 5.3.3 requiring either or for the Exhibits.

c. Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)
   8x8 has completed the CSA Star Assessment.

c. Completion CSA Star Continuous Monitoring. (5 points)
   8x8 agrees to complete the CSA STAR continuous Monitoring assessment prior to award.

Cloud Security Alliance > STAR Registry > STAR Registrant - 8x8, Inc

8x8, Inc

8x8 business VoIP helps you serve your customers better with mobile, flexible solutions that help you do business anywhere, anytime. From hosted VoIP business phone service and cloud-based call center software to unified communications, our services are easy to use, incredibly advanced and less expensive than traditional solutions. Ranked #1 hosted VoIP provider. Proven. Reliable. Secure.

Added: July 5th, 2018

8x8

STAR Self-Assessment

Submitted: July 5th, 2018

Consensus Assessments Initiative Questionnaire v3.0.1	Download

8.14 (E) SERVICE PROVISIONING

8.14.1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

Installation schedules will vary due to size and scope of the project however emergency or rush services are available. There may be a fee associated for outside the normal deployment timeframe.

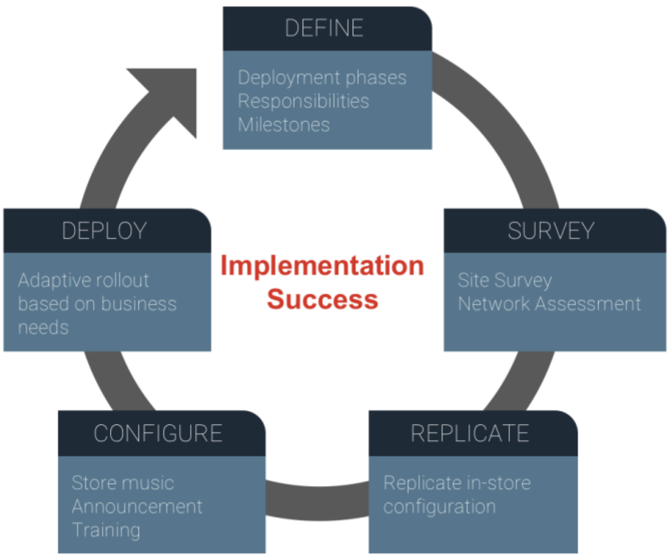
Porting of numbers is typically the greatest delay and is reliant upon other carriers to release the numbers. 8x8 has a dedicated team to manage this implementation process. Net new deployment can be rushed if necessary from a few days to a week dependent upon cooperation of the third party releasing the numbers.

8.14.2 Describe in detail the standard lead-time for provisioning your Solutions.

The standard lead time necessary for provision the 8x8 solution can vary dependent on multiple factors as listed below. Our average provisioning should only require a few weeks to provision the solution for the Purchasing Entity. At 8x8 we use the methodology outlined below to ensure the services we provide are provisioned correctly from the beginning to ensure a successful implementation.

Provisioning factors which impact the lead time:

- Complexity of the Purchasing Entities environment.
- Is the solution unified voice communications or is contact center being implemented as well?
- Size and scale of the deployment such as multiple locations.



8.15 (E) BACK UP AND DISASTER PLAN

8.15.1 Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

Customers can generally individually prescribe retention periods and disposition requirements. Generally, those requirements are provided to 8x8 throughout the course of the business relationship.

8.15.2 Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

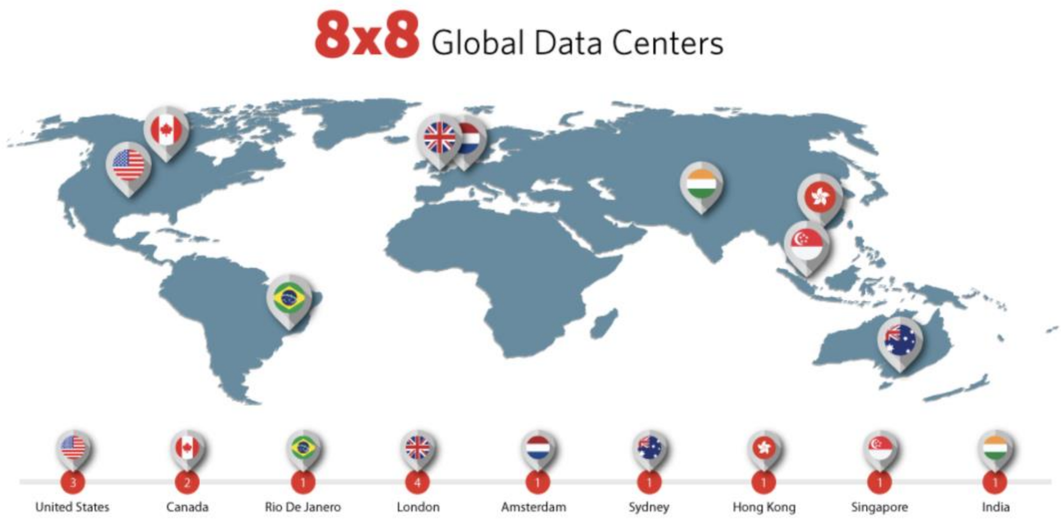
Disaster Recovery and Business Continuity planning focuses on the recovery and restoration of an IT system following a disruption. This Disaster Recovery and Business Continuity Plan (DR/BCP) ensures that primary business essential functions and services continue to be performed during a wide range of emergencies, service disruptions or catastrophic events. 8x8 Disaster Recovery and Business Continuity plans are updated and tested annually for all IT systems in accordance with NIST SP 800-34 Rev1, “Disaster Recovery and Business Continuity Planning Guide for Information Technology Systems.

Disaster Recovery and Business Continuity planning generally includes one or more of the following approaches to restore disrupted services:

- Restoring information systems using alternate equipment;
- Performing some or all of the affected business processes using alternate processing (manual) means (typically acceptable for only short-term disruptions);
- Recovering information systems operations at an alternate location (typically acceptable for only long-term disruptions or those physically impacting the facility); and
- Implementing appropriate NIST 800-53 R3 Disaster Recovery and Business Continuity planning controls based on the information system’s FIPS 199 security impact level.

8.15.3 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.

We own and manage our own software and hardware. We only contract only with highly secure top tier data centers. We place additional contractual requirements on these data centers to not only meet SSAE 16 SOC I and SOC II but also our minimum-security standards of administrative, technical and physical safeguard standards to and maintain the confidentiality, integrity and availability of these systems. For high availability all of our systems have no single points of failure and, for instance, in the U.S. we can fail over core call flow over from West to East coast data centers in 30 seconds.



8.16 (E) HOSTING AND PROVISIONING

8.16.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

8x8 secure hosted voice and collaboration services are offered as SaaS. All cloud services and applications are configured to specifications according to customer requirements. This requirement would not be applicable to our offering.

8.16.2 Provide tool sets at minimum for:

1. Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)
   This is not applicable to 8x8 due to our secure hosted voice and collaboration services are offered as a SaaS service.

2. Creating and storing server images for future multiple deployments
   This is not applicable to 8x8 due to our secure hosted voice and collaboration services are offered as a SaaS service in the public cloud resources are sized and adjusted automatically based on users quantity.

3. Securing additional storage space
   This is not applicable to 8x8 due to our secure hosted voice and collaboration services are offered as a SaaS service. 8x8s SaaS offering is multi-tenant and resources adjust automatically to scale based upon the number of active users.

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).
   Monitoring tools are inherently integrated into the 8x8 UCaaS platform and are a part of the SaaS offering in this RFP

8.17 (E) TRIAL AND TESTING PERIODS (PRE- AND POST- PURCHASE)

8.17.1 Describe your testing and training periods that your offer for your service offerings.

8x8 Elite Touch Implementation Services for Virtual Office and Virtual Contact Center help accelerate successful deployments for any size business and for any level of complexity. These services provide pre and post purchase options to ensure successful deployments.

Pre-purchase we recommend Purchasing Entities utilize our free Online Testing Utility which will open a socket-connection to your browser and pass simulated VoIP Traffic to your home/office computer. This test measures the quality and performance of your Internet connection between your home/office network and the 8x8 servers. The network viability is necessary to ensure good connectivity for VOIP communications.

Our supportive sales teams and engineers will help Purchasing Entities realize the fastest time to value—from single site deployments to large and complex requirements that typically involve multiple sites, global implementations and integration with multiple back-end systems.

For solid and successful implementations 8x8 understands the importance of training. We make learning simple no matter what time zone you reside in or what 8x8 product you need to learn, we support your training needs. 8x8 offers free online trainings for the end user as well advance trainings or certifications delivered virtual or live for an additional cost.
Free Online:
Immediate access to elegantly designed self-paced training is available 24/7 on the 8x8 Academy website: https://www.8x8.com/8x8-academy/free-online-training

- Virtual Office End User
- Virtual Office Administrator
- Virtual Contact Center
- ContactNow

Fee Associated Training Options:
These options are applicable to training the level of user; End User, Agent or Supervisor. More information is available : https://www.8x8.com/8x8-academy/end-user-training.

- Virtual Office Adoption Kit
- Virtual Office Remote Training
- Virtual Office On-Site Training
- Virtual Contact Center Adoption Kit
- Virtual Contact Center Remote Training
- Virtual Contact Center On-Site Training

8.17.2 Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

8x8 offers participating entities test environments in which they are able to test and evaluate our solution in their environment for proof of concept. This would be offered in the form of a demo or a small, non-customized, short-term evaluation of the 8x8 services.

Or

The participating entities may choose to utilize our Pilot Migration option to test and evaluate our services in the participating entities environment. These pilots can be configured and customized to meet the individual customer needs. The times necessary for the Pilot Migration testing will vary on the size and scope of the project. This testing and evaluation option resembles the traditional 8x8 on-boarding processes.

8.17.3 Offeror must describe what training and support it provides at no additional cost.

8x8 offers many options of free online trainings for the end user:
Immediate access to elegantly designed self-paced training is available 24/7 on the 8x8 Academy website: https://www.8x8.com/8x8-academy/free-online-training

- Virtual Office End User
- Virtual Office Administrator
- Virtual Contact Center
- ContactNow

8.18 (E) INTEGRATION AND CUSTOMIZATION

8.18.1 Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

8x8 amplifies team productivity and enhances customer service with built-in integration with apps such as Salesforce, NetSuite, Desk.com, Skype for Business, Microsoft Outlook and Office 365. 8x8 also uniquely unifies communications and contact center capabilities.

8.18.2 Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

8x8 UCaaS platform is inherently designed for enterprise class customers like the Purchasing Entity thus the ability to customize their needs within their environment. Additionally we offer API solutions which further enable customizations.

8.19 (E) MARKETING PLAN

Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

8x8 will strive to ensure our go to market strategy is robust and comprehensive reaching the all verticals of government who have the opportunity to purchase through the Master Agreement or a Participating Addendum.

Messaging:

8x8 will strive to focus our Marketing Strategy & Objectives to partner with NASPO ValuePoint to provide great customer service in addition to providing the best Cloud Solutions in communications and collaboration to the Participating Entities of NASPO ValuePoint.

Planning initiatives:

- Identify prospects
- Communication plan – messaging
- Collateral development – appeal to public sector
- Event planning to participate in public sector conferences
- Planning of industry events in field
- Outreach via social media awareness campaigns
- Press release upon award and contract finalization
- Education and training for internal organization at 8x8 – evangelizing in the field
- Brand Identity Creative – Public Sector Focus
- Public sector event participation
- Outbound call out campaign

We will utilize our website as a key marketing tool which extends the sales reach via product and solution collateral, opt-in mailings, and webinar campaigns to drive knowledge and awareness of new offerings. We will establish in our government portal on our website information pertaining to NASPO ValuePoint and drive awareness campaigns around messaging contract award.

Field Marketing:

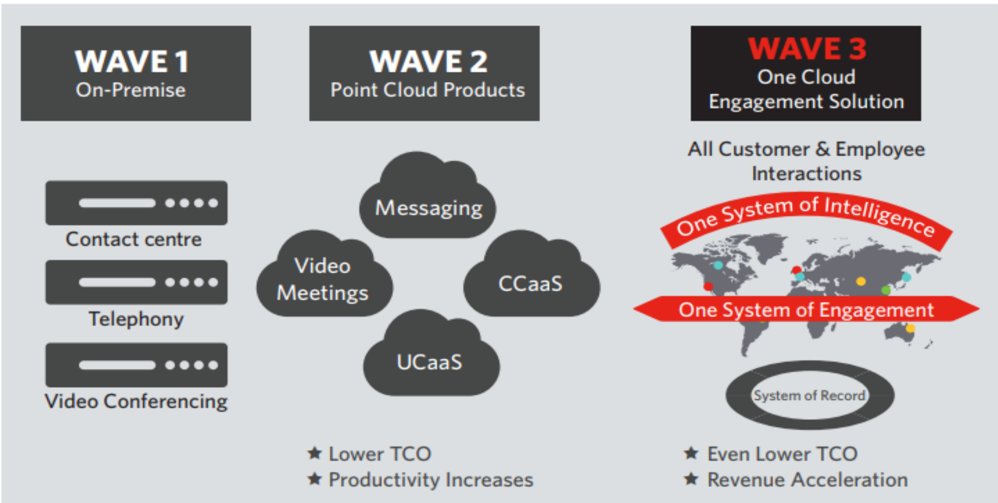
- We will be utilizing our inside sales team, to manage lead generation, pre-sales support, product quotations and post-sales customer support.
- Event participation
- Partnering with business partners who are NASPO ValuePoint contract holders – teaming

- Field efforts will include field sales resources which will be equipped with relevant case studies and product training material
- Market leading product portfolio designed to span a wide range of government entities.
- 8x8 has been working closely with the public sector many years and has referenceable government customers we will work with to build awareness through case studies.

8.20 (E) RELATED VALUE-ADDED SERVICES TO CLOUD SOLUTIONS

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.

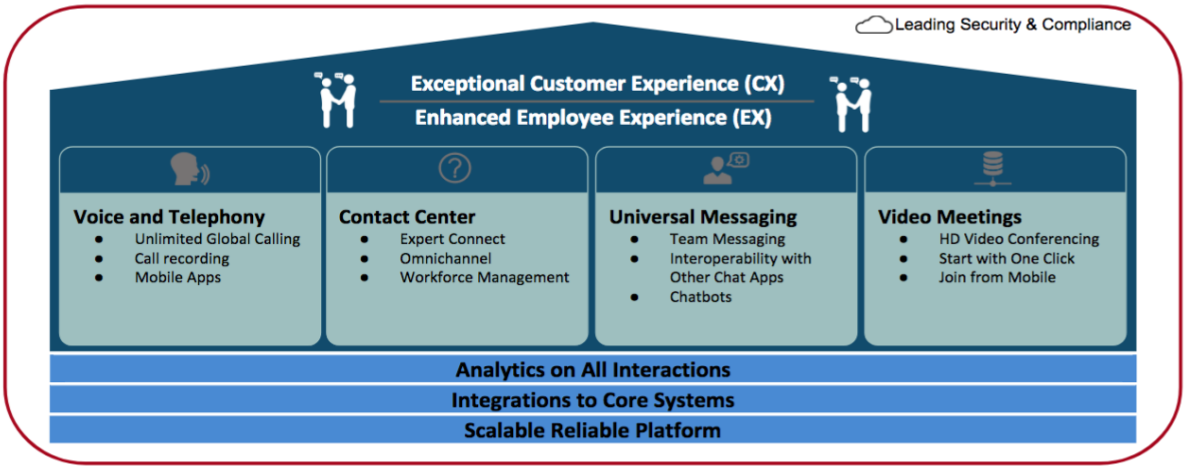
The 8x8 solution will optimize valuable moments of engagement with one set of data in one system of intelligence. This means faster time to resolution at a lower cost, and a better experience for customers and employees. The following graphic depicts how 8x8 is taking unified communications to a new level and ensuring valued-added services as part of an awarded contract with NASPO ValuePoint.



8x8 X Series transforms the customer experience by providing the enterprise with the ability to intelligently and quickly collaborate across any channel and easily access the company's most critical data, analysis and experts. With customer and employees interacting in one system of engagement, enterprises can now optimize valuable moments of engagement with one system of intelligence. X Series accelerates your company's' ability to innovate, respond and serve customers and results in an exceptional experience for both employees and customers.

8x8. The experience is everything.

- X is an easy transition from collaboration to phone to meeting.
- X is full context with every live interaction.
- X is centralized team messaging with all collaboration platforms.
- X is data analytics on every employee and customer interaction.
- X is supervisor enablement and agent feedback.
- X is intelligent interactions between employees and customers



8.22 (E) SUPPORTING INFRASTRUCTURE

8.22.1 Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

8x8 recommends the Purchasing Entity to work with an 8x8 engineer to run the 8x8 Network Utility on all your networks where you would use an 8x8 endpoint. This helps diagnose most common network issues.

If you have a use case that requires the use of the 8x8 Virtual Office desktop app or Virtual Office mobile app over Wi-Fi, you must run the utility on your wireless network as well. If phones are on a separate VLAN, and the Virtual Office apps are on a different VLAN, engineers want to ensure to run the test on all applicable VLANs.

Network

Parameters	Requirements
Wiring	At least Cat 5 (preferably Cat 6) wiring to each user
PoE (recommended)	For details, please refer to PoE requirements for: n Polycom n Yealink n Cisco
Packet loss	0% packet loss
Jitter	<20 ms jitter

Network latency	<100 ms latency to 8x8 data centers. VoIP services are known to work even in higher latency conditions up to 150-200 milliseconds. However, this must be maintained consistently with no packet loss.
Bandwidth	n G711 Codec: 90 kbps symmetric/call

Parameters	Requirements
requirement	n G722 Codec: 90 kbps symmetric/call n G729 Codec: 35 kbps symmetric/call Please make sure you have 50% of your available bandwidth free to accommodate any spike in usage. Always assume that at least 35% of your users are on call at any time. However, depending on your company's use case, you may have a higher percentage.
If running a converged network for voice and data	Configure VLANs to separate the traffic. Please ensure that the Phone VLAN has the following DNS and NTP in its DHCP Use 8x8 DNS (Global Traffic Managers) servers 192.84.18.11 and 8.28.0.9 Use 8x8 NTP server ntp.packet8.net **Note:** The recommended DNS and NTP do not resolve any other domain except 8x8.com and packet8.net.
Quality of Service (QoS) and traffic shaping	Configure on premises to prioritize voice traffic specific to 8x8 IP ranges on all UDP and TCP ports. Please defineegress QoS.
QoS for Wi-Fi	If the majority of your users are on Wi-Fi rather than Ethernet, please make sure you follow the best practices in Wi-Fi deployment to ensure plenty of coverage.
Local DNS consideration	If you use DNS situated on the LAN, please make sure that you are using local Internet service providers as your forwarders.
DHCP scope	Ensure that there are no rules specified to force any provisioning server or NTP server to deviate from default 8x8 values. For example: n For provisioning servers, you must disable Option 66. n For NTP servers (other than 8x8 NTP servers), you must disable Options 4 and 42.

VPN use cases	If your remote users or Internet egress use a VPN tunnel, please make sure that the 8x8 traffic does not traverse it. You need to consider a Split Tunnel to have local Internet egress for 8x8 traffic. In addition, split DNS to resolve 8x8 domain queries locally. Speak to your 8x8 engineer for more

Parameters	Requirements
	information.
WAN failover	We highly recommend that you use dual WAN connections in a failover state by using WAN link redundancy. Dual WAN connections in load balancing are not supported.
Maximum Transmission Unit (MTU)	The network must support an MTU of 1500 bytes per packet. The MTU is the size of the largest protocol data unit that the layer can pass onward.
UDP protocol priority	High
Stateful Packet Inspection (SPI)	Disabled
ALG/Helper and UDP flood detection	Disabled: For details, please refer to our page on ALG and how to disable it.

Subnets

We recommend that you allow outbound traffic to the following 8x8 subnets through your firewall, and have all ports open to 8x8 subnets. Traffic from any IP port on your internal LAN to any IP port on 8x8's secure subnets is outbound only.

Zones	Subnets
US West Coast	n 192.84.16.0/22 n 162.221.236.0/23 n 8.5.248.0/23

Zones	Subnets
	n 63.209.12.0/24

US East Coast	▪ 8.28.0.0/22 ▪ 162.221.238.0/23

Firewall Ports

If you want to allow access port-by-port rather than by allowing access to subnets, please refer to the following lists of ports and the traffic they support. Note that, if you have enabled access to subnets, you do not need to enable ports individually.

The following customer firewalls must allow both outbound TCP and UDP traffic for 8x8 services to function. Generally, traffic is allowed by default by all firewalls.

Traffic Types	TCP and UDP Ports
SIP signaling	UDP and TCP 5196-5199 (5199 Primary)
Registration	UDP and TCP 5060-5061 (5060 Primary)
8x8 activation service	UDP and TCP 5299 and 5399
DNS	UDP and TCP 53

The following customer firewalls must allow outbound UDP traffic for 8x8 services to function. Generally, traffic is allowed by default by all firewalls.

Traffic Types	UDP Ports
Polycom phones	UDP 2222-2269
Cisco Linksys SPA and ATA	UDP 16384-16538
Aastra phones	UDP 3478-3480 (3479 Primary)
Panasonic DECT	UDP 16000-20000
Obihai ATA	UDP 16600-18398
AudioCodes ATA	UDP 6000-6230
Yealink and Yealink DECT	UDP 11780-12780
Virtual Office mobile app	UDP 5199
NTP	UDP 123
8x8 applications	UDP 5401

8x8 applications	n UDP 24000 to 30999 RTP for voice/video n UDP 38000 to 44999 RTP for voice/video n UDP 52000 to 58999 RTP for voice/video n UDP 50000 to 65535 RTP for Virtual Office meeting video
Virtual Office desktop app with advanced audio codec	UDP 30000-30040
8x8 Network Diagnostics and Network Monitoring Tools	UDP 3478-3480
BPA	UDP 15044

The following customer firewalls must allow outbound TCP traffic for 8x8 services to function. Generally, traffic is allowed by default by all firewalls.

Traffic Types	**TCP Ports**
Switchboard Pro	n TCP 15000 n TCP 20080-23080 n TCP 2098-2130
Virtual Office desktop app	n TCP 80 (HTTP) n TCP 443 (RTPM or HTTPS)

Traffic Types	**TCP Ports**
	n TCP 8443 (HTTPS Exchange/Gmail) n TCP 23960 (Click2Pop)
LDAPS for Corporate Directory	TCP 636
Salesforce plug-in	TCP 2097-2601
Act! plug-in	TCP 2099
Virtual Office desktop and online app XMPP	TCP 5222
SRTP for IP phone	TCP 5443
SRTP for Virtual Office desktop app	TCP 5401
8x8 applications	n TCP 5960 n TCP 9443 n TCP 16443 n TCP 8243

Virtual Office Apps and Meetings

Parameters	Requirements
Operating systems	n Windows 7 or newer, with: ◦ 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor ◦ 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit) ◦ 16 GB of available hard disk space (32-bit) or 20 GB (64-bit) ◦ DirectX 9 graphics device with WDDM 1.0 or higher driver n Mac OS 10.9 or newer: Mavericks (10.9), Yosemite (10.10), El Capitan (10.11), or Sierra (10.12)
Browsers	n Internet Explorer® 9.0 or newer n Google Chrome 5.0 or newer n Firefox® 2.0 or newer n Safari™ 3.0 or newer

Parameters	Requirements
Bandwidth	Minimum 1.5 Mbps down/up (Cable modem, DSL, or better)
Other	Headset with microphone

Depending on which platform you are using, you will have to tag your SIP and RTP packets differently.

Platform	SIP	RTP
Windows (normal user)	0xA0 (DSCP 40, CS5)	0xE0 (DSCP 56, CS7)
Windows (admin user)	0x68 (DSCP 26, AF31)	0xB8 (DSCP 46, EF)
Mac/iOS (pre-iOS 10/Sierra)	0x68 (DSCP 26, AF31)	0xB8 (DSCP 46, EF)
Mac/iOS (iOS 10/Sierra+)	0x68 (DSCP 26, AF31)	0xB8 (DSCP 46, EF)
Android	0x68 (DSCP 26, AF31)	0xB8 (DSCP 46, EF)
Polycom	0x68 (DSCP 26, AF31)	0xB8 (DSCP 46, EF)

8.22.2 If required, who will be responsible for installation of new infrastructure and who will incur those costs?

8x8 does not install new infrastructure to support our services and solutions. However, we work with many authorized partners who provide these services in upgrading the network to meet VOIP solution standards. 8x8 only works with authorized partners who must sign strict partnering agreements with 8x8 and understand these requirements of the network infrastructure to support our solutions.

Network infrastructure costs associated as stated in the tables above are the responsibility of the Purchasing Entity.

ATTACHMENT E: CONTRACTOR SERVICES USE POLICY

I. Definitions. Capitalized terms used and not defined herein shall have the meanings assigned to them in the document to which this Use Policy (this "**Policy**") applies (the "**Terms**").

II. Scope of Purchasing Entity Responsibility. Purchasing Entities (or any other party receiving access to Contractor's Services under the Master Agreement, including but not limited to the Lead State and Participating Entities, which for purposes of only this Use Policy shall be inclusive in the term, "**Purchasing Entities**") shall be responsible for ensuring compliance with this Policy by the parties specified herein, and any violation of this Policy by any such party shall constitute and be considered a breach hereof by Purchasing Entity itself. Without limiting the foregoing, Purchasing Entity shall be responsible and liable for all accessing and/or use of the Contractor Services or the Contractor platform by or on behalf of it, its Agents, or other users of such Services, other than unauthorized activities resulting from the gross negligence or willful misconduct of Contractor or its Affiliate or Partner ("**Purchasing Entity Use**").

III. Determination of Requirements. Purchasing Entity shall be solely responsible for determining and familiarizing itself with – and seeking its own legal counsel regarding – all United States, foreign international, national, state, provincial, territorial, municipal, local, or other laws, regulations, codes, ordinances, treaties, conventions, writs, decrees, resolutions, promulgations, or court or administrative orders or rulings ("**Laws**"); contractual obligations; Foreign Requirements; network/wireless carrier requirements; and industry-standard frameworks (such as the Mobile Marketing Association Guidelines in the case of texting) (collectively, "**Requirements**") that might apply to Purchasing Entity Use or the use and/or transport of any applicable equipment, which such Requirements might include without limitation domestic and/or foreign Laws relating to:

(i) the import or export of goods, equipment, technologies, data, or other materials;

(ii) marketing, solicitation, business practices, or telecommunications or electronic communications (collectively, "**Marketing Laws**"), such as the US Telephone Consumer Protection Act of 1991 (the TCPA) (which significantly restricts telephone solicitations (i.e., telemarketing) and the use of automatic dialing systems, artificial or pre-recorded voice messages, SMS text messages, and facsimile communications) and Canada's Anti-Spam Legislation (CASL);

(iii) privacy, or the security or protection of personal data or other categories of data ("**Data Protection Laws**"); and

(iv) surveillance; the monitoring or recording of conversations, communications, or other activities; or wiretapping ("**Monitoring Laws**"), which such Laws may require advance notice or consent for such activities and may be implicated by certain uses or features of the SaaS Services, such as Barge-Monitor-Whisper and Quality Management (which allows certain Agents to monitor other Agents' computer activities).

Contractor shall have no obligation to provide legal advice of any kind to the Purchasing Entity Parties, and the Purchasing Entity Parties shall not treat or rely on any statements, communications, or materials of the Contractor Parties as such.

IV. Use Outside of United States. Because the Services are nomadic, they are potentially accessible from virtually anywhere in the world, including outside of the United States. While the Master Agreement does not prohibit Purchasing Entity Use outside of the United States, Contractor makes no representations, warranties, or guarantees regarding the compliance of Purchasing Entity Use with prohibitions or restrictions imposed by Law, carriers, ISPs, etc. outside of the United States ("**Foreign Requirements**"), and Purchasing Entity shall be solely responsible for ensuring compliance therewith, regardless of any consent by Contractor or its Affiliate to such Purchasing Entity Use.

V. Policy Requirements. Purchasing Entity agrees, represents, warrants, and covenants the following:

(a) ***Legal and Other Compliance –*** All Purchasing Entity Use, and all use and transport of any equipment ordered from Contractor by or on behalf of Purchasing Entity or its Affiliate in connection with the Services, shall comply with all applicable Requirements.

(b) ***Consents, Etc. –*** Purchasing Entity has obtained all consents, licenses, rights, authorizations, and/or permits and has provided all disclosures and notices/notifications required (including without limitation under Marketing, Data Protection, or Monitoring Laws) for or in connection with Purchasing Entity Use or related to Registration Information or any personal data therein.

(c) ***Do-Not-Call List –*** To the extent that Purchasing Entity Use might involve telemarketing, solicitation, or substantial outbound activities, Purchasing Entity shall maintain and enforce an accurate, comprehensive, and up-to-date internal “do not call” list to prevent contacting parties that do not wish to receive further communications.

(d) ***No Resale –***Services shall not be sold/resold, leased/subleased, licensed/sublicensed, or otherwise made available to any other third party (other than an Affiliate of Purchasing Entity), and all orders under any Participating Addendum and all Purchasing Entity Use shall be for Purchasing Entity or its Affiliate’s own internal business use.

(e) ***Documentation –*** All Purchasing Entity Use shall be consistent with the applicable documentation shared as part of the RFP process or any other submission by Contractor to the Lead State (the, “**Documentation**”).

(f) ***Order of Equipment –*** Purchasing Entity shall order any equipment to be used with the Services solely for such use.

(g) ***No Bribery –*** Neither the Purchasing Entity Parties nor any Agent or other user has received or been offered any bribe, kickback, or illegal or improper payment, gift, or thing of value from any Contractor Party in connection with a Participating Addendum.

(h) ***Other Prohibited Uses and Activities –*** In no event shall Purchasing Entity Use consist of, involve, promote, or faciliate any:

- (i) fraudulent, criminal, defamatory, harassing, unlawful, or tortious conduct or activity;
- (ii) transmission of misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value;
- (iii) transmission, storage, or distribution of any virus, time bomb, Trojan horse, worm, malware, spyware, or similar programs, or files, code, or other materials containing any of the foregoing;
- (iv) breach, violation, or infringement of any intellectual property, privacy or other right – or misappropriation of the property – of any party;
- (v) accessing or use of Services in or from a US embargoed country;
- (vi) any conduct or activity that might cause Contractor or any of its Affiliates or Partners to violate any Law.

(i) ***Export Control –*** At no point during the Term of the Master Agreement or any subsequent period during which Purchasing Entities, its Affiliates, and/or the Agents or other users continue to have access to Contractor Services (the “**Access Period**”) will any of the foregoing parties be named on any US government denied-party list.

(j) ***Reasonable Business Use –***Services shall be used solely for reasonable business use, which, in the case of “unlimited,” “Editions,” or X Series plans, features, or functionalities, shall be limited to three times (3X) the average monthly usage of the same Services by all customers of Contractor.

(k) ***Accurate Registration Information –*** All Registration Information shall be accurate, current, and complete at all times during the Access Period. Purchasing Entities shall promptly update Registration Information as needed to ensure its accuracy and shall promptly verify any Registration Information upon reasonable request from Contractor.

(l) ***Use With Supported Devices –*** All Purchasing Entity Use (other than via an 8x8 desktop or mobile application) shall be via equipment then-listed as supported by Contractor at www.8x8.com/CommunicationsSolutions/Equipment (“**Supported Devices**”) or approved in advance in writing by Contractor (not to be unreasonably withheld) for such Purchasing Entity Use. Regardless of any such approval, Contractor shall have no liability for or obligation to support such Purchasing Entity Use with/through any equipment that is not a Supported Device.

(m) ***Security of Ordered Products –*** Purchasing Entity shall, during the entire Access Period, (i) implement and maintain reasonable and appropriate measures and safeguards to prevent unauthorized access to and/or use of the Services and/or the related account(s); data transmitted, received, or stored therein or therethrough; and any equipment used to access any of the foregoing and (ii) promptly provide notice to Contractor of any such unauthorized access or use or other breach of any of the foregoing (including without limitation any loss or theft of such equipment) and provide such cooperation as Contractor might reasonably request to address or prevent any such incident. Without limiting the foregoing, Purchasing Entity shall (1) instruct, train, and oversee all Agents as necessary to ensure that they (yy) choose robust password combinations, change their passwords regularly, and not disclose their passwords except to authorized Contractor support agents and (zz) perform a “log off” / exit from such accounts at the end of each session of access thereto and (2) not modify the aforementioned equipment in any manner without Contractor’s prior express written consent.

(n) ***SaaS Services Updates and Security –*** Throughout the Access Period, Purchasing Entity, its Affiliates accessing or using Services, and the Agents and other users shall (i) promptly install all upgrades, bug fixes, patches, and other corrections relating to the Services made available by or on behalf of Contractor or its Affiliates or Partners and (ii) not take any action or omission that might reasonably be expected to (A) disrupt or compromise the integrity or security of any services, platforms, or networks of Contractor or its Affiliates or Partners, (B) cause material damage to Contractor, its Affiliates or Partners, or any customer of Contractor, its Affiliates, or any their Partners, or (C) compromise the privacy of any such customer.

(o) ***Emergency Services and High-Risk Applications –*** THE SERVICES SHALL NOT – AND PURCHASING ENTITY UNDERSTANDS THAT THE SERVICES ARE NOT INTENDED TO – BE USED FOR, ANY APPLICATION (SUCH AS CARRYING AN ALARM SIGNAL) WHERE FAILURE, INTERRUPTION, OR MALFUNCTION MAY REASONABLY BE ANTICIPATED TO RESULT IN BODILY INJURY, LOSS OF LIFE, OR SUBSTANTIAL DAMAGE TO PROPERTY. Purchasing Entity shall inform Agents and other users and keep them apprised of any limitations of the Services with respect to contacting emergency services of which Contractor or its Affiliates or Partners notify Purchasing Entity.

(p) ***Prohibited Acts –*** During the Access Period, neither the Purchasing Entity Parties nor the Agents or other users shall:

(i) inspect, possess, use, copy, reverse engineer or attempt to discover the source code of any program or other component of the Services or Contractor Platform or any source code used to create any such program or other component, except as expressly permitted by applicable law;

(ii) attempt to hack or gain unauthorized access to any network, environment, or system of Contractor, its Affiliates or Partners, or any customer of Contractor, its Affiliates, or their Partners;

(iii) access or use any Services in order to build a competitive product or for the primary purpose of monitoring its availability, performance, or functionality, or for benchmarking or competitive purposes; or

(iv) trunk or forward any extensions or numbers associated with the Services to a private branch exchange or key system or to other numbers that can process multiple calls simultaneously.

(q) ***Oversight of Agents –*** Purchasing Entity shall (i) ensure that each Contractor Virtual Office extension (other than Conference Extensions) and each log-in associated therewith is accessed and used solely by the Agent then-assigned to such extension, (ii) not designate as an Agent any individual over whom Purchasing Entity lacks sufficient control (contractual or otherwise) to ensure compliance with this Policy or allow any such individual to access or use Services, and (iii) during the Access Period, instruct, oversee, and train the Agents, other users, and its workforce and Partners as necessary to ensure Purchasing Entity's compliance with this Policy.

VI. Indemnification and Suspension.

(a) ***Indemnification*** – Purchasing Entities shall (i) defend Contractor, its affiliates, and their personnel (collectively the "**Contractor Parties**") from and against any action, claim, demand, suit, investigation, inquiry, or proceeding (each a "**Claim**") threatened or brought against any of them by any party that arises out of or results from any Purchasing Entity's Content or any actual or alleged breach of this Use Policy by Purchasing Entity and (ii) indemnify and hold harmless the Contractor Parties against any losses payable by any of them pursuant to the adjudication or settlement of any such Claim.

(b) ***Suspension*** – Where a Purchasing Entity breaches this Use Policy, Contractor may suspend the Services without affording the applicable aggrieving party a cure period and/or place reasonable limitations or restrictions on the use of any Services that are being used by a Purchasing Entity in violation of this Use Policy under the terms of the Master Agreement. No such action by Contractor shall relieve a Purchasing Entity of any of its obligations under the Master Agreement.