



Contract #: AR3111

## STATE OF UTAH COOPERATIVE CONTRACT

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

NWN Corporation

Name

271 Waverley Oaks Road

Street Address

Waltham

MA

02452

City

State

Zip

Vendor # VC226515 Commodity Code #: 920-05 Legal Status of Contractor: For-Profit Corporation

Contact Name: Mathew S. Niemann Phone Number: 916-637-2135 Email: MNiemann@nwnit.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: Monday, April 01, 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: Service Offering EULAs, SLAs

**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:

- All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
- 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

Richard E. Johnson

Richard E. Johnson (Apr 4, 2019)

Apr 4, 2019

Contractor's signature

Date

### DIVISION OF PURCHASING

Christopher Hughes

Christopher Hughes (Apr 4, 2019)

Apr 4, 2019

Director, Division of Purchasing

Date

Richard E. Johnson CFO

Type or Print Name and Title



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

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

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

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

**Contractor** means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Master Agreement.

**Data** means all information, whether in oral or written (including electronic) form,

---

<sup>1</sup> A Sample Participating Addendum will be published after the contracts have been awarded.

<sup>2</sup> The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and SaaS.

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), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

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

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

**Statement of Work** means a written statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

**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.

**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.

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

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

**8. Confidentiality, Non-Disclosure, and Injunctive Relief**

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity's or Purchasing Entity's clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason

to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, 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 shall be an event of default under this Master Agreement:

- (1) Nonperformance of contractual requirements; or
- (2) A material breach of any term or condition of this Master Agreement; or
- (3) Any certification, representation or warranty by Contractor in response to the



solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

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

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

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

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

(1) Exercise any remedy provided by law; and

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

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

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

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

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

**12. Force Majeure:** Neither party shall be in default by reason of any failure in

performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

### **13. Indemnification**

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, 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 performance under the Master Agreement.

b. 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 ("Indemnified Party"), 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; or

(d) It would be reasonably expected to use the Product in combination with such product, system or method.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and

reasonably investigates and defends any Intellectual Property 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 Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor 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 Intellectual Property 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.

**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	<b>Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions</b> 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.

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

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

## **19. Ordering**

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

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

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

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

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

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

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

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

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

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

## **20. Participants and Scope**

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

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

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

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

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

---

<sup>3</sup> 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.

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

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

Contractor may not share a Purchasing Entity's 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 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.

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

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

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

**27. Administrative Fees:** The Contractor shall pay to NASPO ValuePoint, or its

assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

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

**28. System Failure or Damage:** In the event of system failure or damage caused by Contractor or its Services, the Contractor agrees to use its 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.

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.

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.

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 no additional cost to the Purchasing Entity. 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, 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 principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

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

### **37. Governing Law and Venue**

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

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

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

d. This section is also not a waiver by the Participating State of any form of immunity,

including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

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

**1. Data Ownership:** The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

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 a 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. 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 ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information 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. 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 data 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 shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any 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. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.
- 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 information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

**3. Data Location:** The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. 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, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing 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 to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

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, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by 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 within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall immediately 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 a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been 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 is a direct result of Contractor's breach of its contractual obligation to encrypt personal data or otherwise prevent its release as reasonably determined by the Purchasing Entity, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications 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:** 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 data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. 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. In the event of a termination of the Master Agreement or applicable Participating Addendum, the Contractor shall implement an orderly return of purchasing entity's data in a CSV or another mutually agreeable format at a time agreed to by the parties or allow the Purchasing Entity to extract its data and the subsequent secure disposal of purchasing entity's data.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase purchasing entity's data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the Contractor shall have no obligation to maintain or provide any purchasing entity's data and shall thereafter, unless legally prohibited, delete all purchasing entity's data in its systems or otherwise in its possession or under its control.

d. The purchasing entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

**8. Background Checks:** Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

**9. Access to Security Logs and Reports:** The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this Master Agreement and applicable Participating Addendum.

**10. Contract Audit:** The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. 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 perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

**12. Change Control and Advance Notice:** The Contractor shall give a minimum forty eight (48) hour advance notice (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.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

**13. Security:** As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

**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 data to that which is absolutely necessary to perform job duties.

**15. Import and Export of Data:** The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

**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 services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

**17. Subcontractor Disclosure:** Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, 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.

**18. Right to Remove Individuals:** The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity 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 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 orders without the Purchasing Entity's consent.

**19. Business Continuity and Disaster Recovery:** The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to 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:** 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. Web Services:** The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

**22. Encryption of Data at Rest:** The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

**23. Subscription Terms:** Contractor grants to a Purchasing Entity 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.

## 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	NWNComm (Hosted Collaboration); Converged Infrastructure (AWS)	NWNComm (Hosted Collaboration); Converged Infrastructure (AWS)	N/A	Private, Public, Hybrid

\*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: NWN Corporation

### 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 an Offeror 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 provides tiered pricing to accompany its named user licensing model, therefore, as user count reaches tier thresholds, unit price decreases.

### Cloud Service Model: Software as a Service (SaaS)

SaaS Minimum Discount % Off

Description	Discount
NWNComm: Collaboration User Subscription Services	8.00%
NWNComm: Cloud Infrastructure Packages	5.00%
NWNComm: TelePresence User Subscription Services	8.00%
NWNComm: Endpoints	8.00%
NWNComm: Telecomm Packages	10.00%
NWNComm: Infrastructure and Service Add-Ons	7.00%
AWS	1.00%
<b>Average SaaS OEM Discount Off</b>	<b>6.71%</b>

### Additional Value Added Services

<u>Item Description</u>	<u>Onsite Hourly Rate</u>		<u>Remote Hourly Rate</u>	
	<u>NVP Price</u>	<u>Catalog Price</u>	<u>NVP Price</u>	<u>Catalog Price</u>
Maintenance Services (Support Services-Technicians and Engineers)-Remote Dispatch Engineer	\$ 177.75	\$ 187.00	\$ 130.25	\$ 137.00
Maintenance Services (Support Services-Technicians and Engineers)-Senior Solutions Engineer	\$ 216.00	\$ 227.25		
Professional Services				
Deployment Services-Service Technician	\$ 65.00	\$ 68.50		
Deployment Services-Solutions Engineer	\$ 178.00	\$ 187.50		
Integration Services, Project Manager or Business Analyst or Developer Analyst	\$ 175.00	\$ 184.25		
Integration Services, Technical Architect (System or Data)	\$ 250.00	\$ 263.25		
Consulting/Advisory Services, Consultant (includes Assessments)	\$ 261.50	\$ 276.00		
Consulting/Advisory Services, Principal Consultant	\$ 286.50	\$ 301.75		
Architectural Design Services	\$ 250.00	\$ 263.25		
Statement of Work Services	\$ 215.00	\$ 226.50		
Partner Services	\$ 250.00	\$ 263.25		
Training Deployment Services	\$ 250.00	\$ 263.25		
Professional Services - Project Coordinator	\$ 145.00	\$ 152.75		
Professional Services - Project Manager	\$ 178.00	\$ 187.50		
Professional Services - Strategic Project Manager	\$ 216.00	\$ 227.50		

### Deliverable Rates

	<u>NVP Price</u>	<u>Catalog Price</u>
NCare MACD RequestPer Device/Month	\$ 120.00	\$ 126.00
NCare MACD RequestContact Center Per Device/Month	\$ 150.00	\$ 157.50
NCare Monitoring Services		
Servers or Blade Systems Per Device/Month	\$ 109.00	\$ 114.50
NCare Monitoring Services		
Appliances/Windows/Linux or Host/VCenter/SAN Controller	\$ 163.00	\$ 171.25



### Attachment C - Pricing Discounts and Schedule

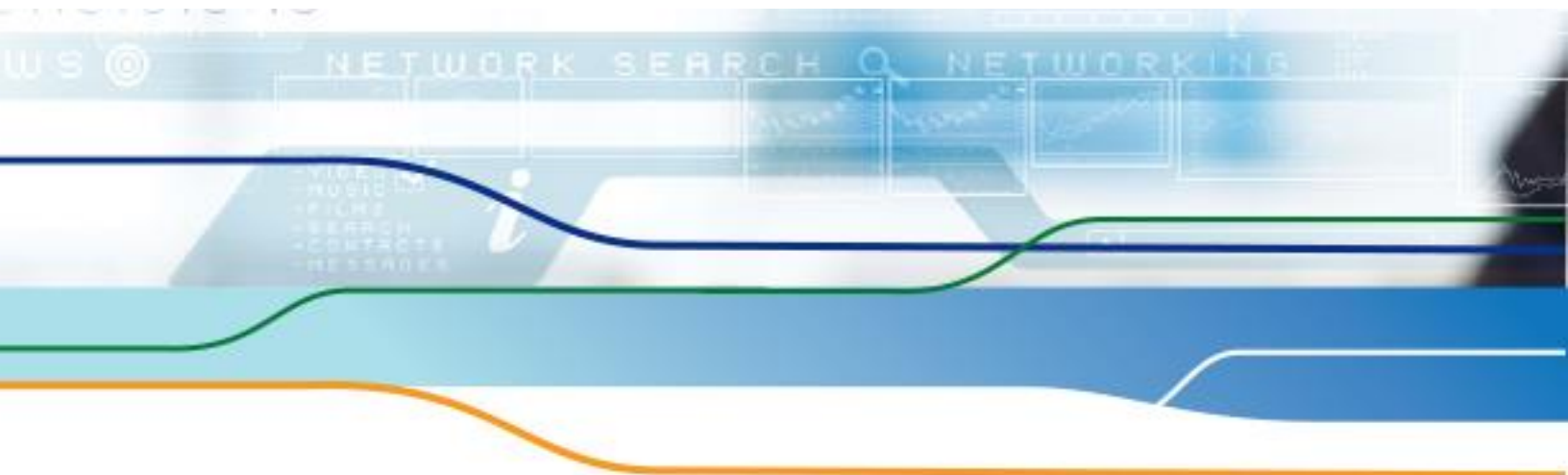
Contractor: NWN Corporation

NCare Management & Monitoring Services				
Servers or Blade Systems Per Device/Month	\$	325.00	\$	341.50
NCare Management & Monitoring Services				
Appliances/Windows/Linux or Host/VCenter/SAN Controller	\$	488.00	\$	512.50
NCare Monitoring Services				
Websites				
Per Device/Month	\$	32.00	\$	33.75
NCare Monitoring Services				
Switches, Gateway, Firewalls, Wireless, Router, SIP/PRI Per				
Device/Month	\$	109.00	\$	114.50
NCare Management & Monitoring Services				
Access				
Per Device/Month	\$	89.00	\$	93.50



# Section 6. NWN Technical Response

RFP No. SK18008 | State of Utah | NASPO Cloud Solutions



# NWN 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.

**NWN Response:** NWN has read and complies with this requirement

NWN Corporation is proud to present our Commercially Available Cloud Computing Solutions that meet the NIST definition of Cloud and are open to all Deployment Models (Private, Public, and Hybrid).

Our proposal includes:

- **NWN Converged Infrastructure:** Full menu of AWS Cloud Services complemented with NWN's Managed Services. Offering includes Cloud Services (Virtualization, Compute, Storage, Networking, Wireless, and Internet-of-Things) from world-leading providers such as Cisco, VMWare, Hewlett Packard Enterprises, and others delivered through Amazon Services and complemented with NWN's Managed Services.

Our Converged Infrastructure Services and Support Services help customers realize the benefits of lower operational costs, higher productivity and greater peace of mind. With practical, cost effective solutions—from data center optimization to cloud computing—solutions are based upon each customer's specific needs and environment, tailored to meet their business and financial objectives.

- **NWN Collaboration, NWNComm:** Full menu/offering of NWN Cloud-Based or Hosted Collaboration Services: Voice, Video, Telecomm, Collaborative Workspaces, Conferencing, and Contact Center Services as well as Advance Application, Dashboard, and Analytic Solutions.

*NWNComm* is a cloud-based/hosted communications platform, which includes voice, video, web conferencing, telecom, and contact center solutions. NWN has the know-how and wherewithal to integrate these essential capabilities with third party applications to create *One Easy-to-Use and Easy-to-Manage Solution*. All *NWNComm*'s Solutions are powered by Cisco Technology, providing *Feature-Rich, End-to-End, Enterprise-Grade Collaboration Solutions* that are hosted in our Geo-Redundant, Secure, and CJIS/SSAE18 Certified U.S. Data Centers and Managed by our Award Winning *NCare* Services.

- **NWN Complimentary Cloud Services:** Workspace Solutions, Monitoring Services, Security Services, Cloud-Based End-Point Security and Performance Optimization Services from NWN and Key Cloud Partners.

NWN focuses on providing applications, content, and data anytime, anywhere, on any device while simplifying operations, improving security, managing costs, and helping businesses to connect. From Virtualized Desktops to Hosted Desktops to End-Point Secure Solutions, we assist customers deploy high-quality, enterprise level desktops improving resources for a monthly or even hourly fee. We work hand-in-hand with each customer to support their ability to securely connect to their employees anywhere, anytime while reducing costs and improving efficiencies.

- **NWN Value Added Services** – Cloud and Security Assessments, Cloud Infrastructure Consulting, IoT Planning, Workspace Solutions, Monitoring Services, Endpoint Security and Performance Optimization, Architecture and Design, and Implementation and Integration Professional Services which are offered on a Project Based (*NPro*) or on an “as needed” based (*NWN Talent Acquisition Services*). We also offer customers our Management and Monitoring Services (*NCare*).

Our Solutions are intended to reduce the IT’s burden. We provide Cloud Transition and Security Assessments, Planning and Design Services, Implementation and Integration Services, and Management and Monitoring Services to support their environments. This allows your IT to have confidence that they have the right solution that enables them to focus on their constituents and initiatives such as Digital Transformation and IoT Initiatives.

## 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](#).

**NWN Response:** Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a share pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.



Our Converged Infrastructure Solution and Complementary Cloud Services meets this requirement.

- **On-Demand Self-Service:** Our service provides customers of all sizes with on-demand access to a wide range of cloud infrastructure services, charging only for the resources you actually use. Consumers can unilaterally provision computing capabilities as needed automatically without requiring human interaction with provider.

- **Broad Network Access:** Our service provides a simple way to access servers, storage, databases, and a broad set of application services over the Internet. We own and maintain the network-connected hardware required for these application services, while customers provision and use what they need via a web application. Connectivity across dedicated WAN and internet is supported though performance requirements of particular use cases may dictate recommended connectivity a particular solution.
- **Resource Pooling:** The environment is a virtualized, multi-tenant environment with security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. For use cases that may require isolated hardware, isolated servers can be provided within a controlled and shared datacenter for services that may have specific security needs.
- **Rapid Elasticity:** Solutions from AWS and other global Cloud Providers provide a massive global cloud infrastructure that allows customers to quickly innovate, experiment, and iterate. Instead of waiting weeks or months for hardware, customers can instantly deploy new applications, instantly scale up as their workload grows, and instantly scale down based on demand. Elastic Load Balancing and Auto Scaling can automatically scale a customer's resources up to meet unexpected demand and then scale those resources down as demand decreases.
- **Measured Security:** Our Converged Infrastructure solutions from AWS and other global Cloud Providers uses automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.



Our **NWNComm Collaboration Infrastructure Solution** meets this requirement.

- **On-Demand Self-Service:** Our *NWNComm* service provides customers of all sizes with on-demand access to cloud-based collaboration services through web-based portals. Consumers can unilaterally provision computing capabilities as needed automatically without requiring human interaction with provider. Our solution includes a Self-Provisioning Portal as well as our menu of *SmartComm* Control, Provisioning, Self-Care Services, Reporting, and Custom Analytics.

- **Broad Network Access:** Our service provides a simple way to access through the network that use standard IP-based data and voice transportation mechanisms. Web-Conferencing tools provide access through the internet. Both services promote use by heterogeneous clients such as: phones, mobile phones including Single Number Reach; tablets, laptops, and desktops with Instant Messaging, Presence, and Collaboration Workspaces; and Video. We own and maintain the network-connected hardware required for these application services, while customers provision and use what they need via a web application.
- **Resource Pooling:** Our service are pooled using a virtualized, multi-tenant environment with security management processes and other security controls designed to isolate each customer from other customers. *NWNComm* leverages a combination of multi-tenancy with multi-customer deployment and redundant datacenters to provide resource pooling per requirement.
- **Rapid Elasticity:** Our *NWNComm* Service provides a cloud infrastructure that allows customers to quickly provision and scale rapidly commensurate with demand appearing to be unlimited to the end user. They system can be elastically provisioned and released as users are added or subtracted. Our *NWNComm* solution, via our *SmartComm* Provisioning tool, provides fast provisioning, and even faster deprovisioning, to meet the customer demand needs, including our Bulk Management tool.
- **Measured Security:** Our *NWNComm* service uses automated monitoring systems to provide a high level of service performance and availability. Features and users can be added as needed. Proactive monitoring is available through a variety of online tools both for internal and external use. *SmartComm* Reporting and Advanced Analytics provide key operational metrics optimization of resources.

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

**NWN Response:** NWN has read the full RFP and complies with Attachment C – NIST Service Models and Attachment D – Scope of Services requirements.

The [National Institute of Standards and Technology \(NIST\)](#) 800-53 security controls are generally applicable to Federal Information Systems. These are typically systems that must go through a formal assessment and authorization process to ensure sufficient protection of confidentiality, integrity, and availability of information and information systems, based on the security category and impact level of the system (low or moderate), and a risk determination.



Our **Converged Infrastructure Solution** and **Complementary Cloud Services** meets this requirement. AWS Cloud services have been validated by third-

party testing performed against the NIST 800-53 controls and are FedRamp Certified.



Our **NWNComm Collaboration Infrastructure Solution** meets this requirement. NWNComm Cloud services have been validated by third-party testing performed against the NIST 800-53 controls and are CJIS and SSAE18 Certified. In addition, our NWNComm solution is based on Cisco Technology which has been validated by third-party testing performed against the NIST 800-53 controls – Cisco also offers these solutions as FedRamp Certified.

- 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**.

**NWN Response:** NWN has read the full RFP and complies with Attachment D – Scope of Services requirements.

**Cloud Services:** NWN's Cloud Services align with NIST requirements and standards.

- **Software as a Service (SaaS)** – NWN provides the capability to customers to our NWN applications running on a cloud infrastructure.
- **Infrastructure as a Service (IaaS)** – NWN provides the capability to customers to provision processing, storage, networks, collaboration, and other fundamental computing resources where customers can deploy and run arbitrary software, which can include OS and applications.
- **Platform as a Service (PaaS)** - NWN provides the capability to customers to deploy onto cloud infrastructure customer-created or customer-acquired applications.

**Cloud Definition:** NWN is a Cloud Provider responsible for making a Service (Converged Infrastructure, Collaboration, and/or Complementary) available. NWN acquires and manages the computing infrastructure required for the Service(s), runs the cloud software required for the Service(s), and make arraignment to deliver the Service(s) to consumers through network access for one hourly or monthly fee.

NWN provides services that meet the five essential characteristics of cloud computing: On-Demand Self Service, Broad Network Access, Resource Pooling, Rapid Elasticity or Expansion, and Measured Services.



- **On-Demand Self-Service:** Our cloud services provide customers of all sizes with on-demand access to a wide range of cloud infrastructure (AWS) and cloud-based collaboration (NWNComm) services without requiring human interaction with provider.
- **Broad Network Access:** Our cloud services provide a simple way to access infrastructure (servers, storage, databases, and a broad set of application services) over the Internet or NWNComm through a network. NWN owns and maintain the network-connected hardware required for these application services, while customers provision and use what they need via a web application. Both services promote use by heterogeneous clients.
- **Resource Pooling:** Our cloud services are pooled using a virtualized, multi-tenant environment with security management processes and other security controls designed to isolate each customer from other customers.
- **Rapid Elasticity:** Our Cloud Services meet this requirement.
  - NWN Converged Infrastructure solutions from AWS and other global Cloud Providers provide a massive global cloud infrastructure that allows customers to quickly innovate, experiment, and iterate Elastic Load Balancing and Auto Scaling can automatically scale a customer's resources up to meet unexpected demand and then scale those resources down as demand decreases.
  - Our NWNComm Service provides a cloud infrastructure that allows customers to quickly provision and scale rapidly commensurate with demand appearing to be unlimited to the end user. Our NWNComm solution, via our SmartComm Provisioning tool, provides fast provisioning, and even faster deprovisioning, to meet the customer demand needs, including our Bulk Management tool.
- **Measured Security:** Our Cloud Services meet this requirement. Both of our Cloud Services uses automated monitoring systems to provide a high level of service performance and availability.

**Deployment Model:** NWN Converged Infrastructure and NWNComm Services provide the ability for our customers to deploy cloud based services through private, public, and hybrid methods.

- **Private Cloud** – NWN provides services where the infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers
- **Public Cloud** - NWN provides services where the infrastructure is provisioned for use by multiple customers.



- **Hybrid Cloud** - NWN provides services where the infrastructure is based on a combination of two or more distinct cloud infrastructures – most commonly a Private/Public Cloud Model.

## 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.

**NWN Response:** NWN intends to provide all of our cloud solutions directly from our geo redundant Datacenters – without the use of Subcontractors to provide cloud solutions. NWN has cloud dedicated practices that meet all requirements listed in RFP.

To help expand our reach, NWN does leverage Resellers Partners who specialize in focusing on specific Markets (example Florida or Higher Education in Southeast). NWN wishes to defer the selection of “Authorized Resellers” (subcontractors) until after contract award and upon execution of each Participating Addendum.

Notwithstanding the foregoing, NWN may allow these Authorized Resellers to offer limited value-added services such as basic installation or training services. NWN understands and agrees that any Authorized Reseller (subcontractor) that it 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.

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.

**NWN Response:** NWN intends to provide all of our cloud solutions directly from our geo redundant Datacenters – without the use of Subcontractors to provide cloud solutions. NWN has cloud dedicated practices that meet all requirements listed in RFP.

To help expand our reach, NWN leverages Resellers Partners who specialize in focusing on specific Markets (example Florida or Higher Education in Southeast). The resellers will be responsible for working with customers to understand our Cloud Solutions and to meet all Administrative, Business and Technical

Requirements of the RFP, as applicable to the Solutions provided. NWN wishes to defer the selection of "Authorized Resellers" (subcontractors) until after contract award and upon execution of each Participating Addendum.

IN addition, NWN has supported small/minority business for decades and will continue to do so on a by Participating Entity basis. Therefore, to ensure the engagement and participation of diverse resellers, including "local" businesses, our reseller selection process aims to objectively select multiple resellers that can best serve the needs of the Participating Entities identified in each Participating Addendum including meeting their SBE/MBE initiatives:

- Based on the Participating State's input and NWN's own business criteria and requirements, NWN will follow its established process for soliciting and selecting appropriately skilled authorized resellers.
- Selected resellers will be expected to (i) "pass" NWN's legal and financial due diligence checks, and (ii) execute a subcontract with NWN and adhere to the terms and conditions of the resulting new contract as well as the respective Participating Addendum.

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.

**NWN Response:** NWN intends to provide all of our cloud solutions directly from our geo redundant Datacenters – without the use of Subcontractors to provide cloud solutions. NWN has cloud dedicated practices that meet all requirements listed in RFP.

Some criteria's include:

- Physical presence within the state;
- Geographic coverage
- Proven historical public sector sales experience and success in the state or geographic location/territory as identified in the Participating Addendum;
- Proven historical understanding and compliance of cooperative contracts;
- Team who comply with contract training requirements; and
- Other value added services that Cisco and/or the Participating Entity may require under that Participating Addendum.

### 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;
- Response times;
- Processes and timelines;
- Methods of communication and assistance; and
- Other information vital to understanding the service you provide.

**NWN Response:** NWN has a documented and proven process for incident management, including data breaches, which meet or exceed industry best practice. NWN has dedicated Contract Managers for each Participating Entity who is responsible for ensuring regular communication, through resolution, to the Participating Entity for major incidents. Below is our standard process.

**Incident Support:** Incidents are escalated based on criticality. Criticality is defined as follows:

Criticality Level	Description
Priority 1 (Critical)	A critical system or service is unavailable.
Priority 2 (Major)	An issue has been detected where functionality is interrupted however there is either a work-around or the service interruption is occurring on a non-critical system or service.
Priority 3 (Minor)	The functionality of a non-critical system or service has been affected. An error has been detected that is easily corrected or is identified as a non-reoccurring or spurious.

- Priority 1 – Dedicated engineer starts process and engages a team of engineers to fix the problem as needed.
  - Vendor escalation immediate. Vendor involvement is agreed upon by both the client and NWN staff based time on constraints and the criticality of the situation.
- Priority 2 and Priority 3 - Client and NWN agree upon an action(s) and escalation plan based upon criticality and resource availability.
  - Customer will designate a list of authorized callers that NWN will validate for security purposed upon opening a new case. It is the customer's responsibility to notify NWN should this contact list change. Notifications should be emailed and all urgent changes should be followed up via a phone call to the command center.
  - NWN maintains support escalation contracts with Cisco, Microsoft, HP, Citrix, and Symantec. These contracts stipulate that NWN will act as 1st and 2nd level support.
  - For all Priority 2 and Priority 3 issues, NWN staff will attempt remediation of issues. Should the issue not be solved within a

reasonable amount of time, NWN will escalate calls to these vendors using its contracts.

- Clients may request that all Level 1 calls be immediately escalated to these vendors.
- NWN will work with other client vendors directly and will coordinate troubleshooting efforts over the phone. It is the client's responsibility to maintain all other vendor escalation contracts with their individual respective vendors. Many vendors require directly purchased support in order to provide 2nd and 3rd level support and code updates.
- It is also the client's responsibility to ensure compliance with individual vendor's requirements regarding version supportability.
- Products that are no longer supported by their respective vendor will be supported by NWN on a "best-effort" basis.
- If NWN can obtain support for these products on a "for-fee" basis, NWN will seek approval for this additional support from the client and will pass all fees associated with such requests back to the client.

#### Incident Management Process Flow:

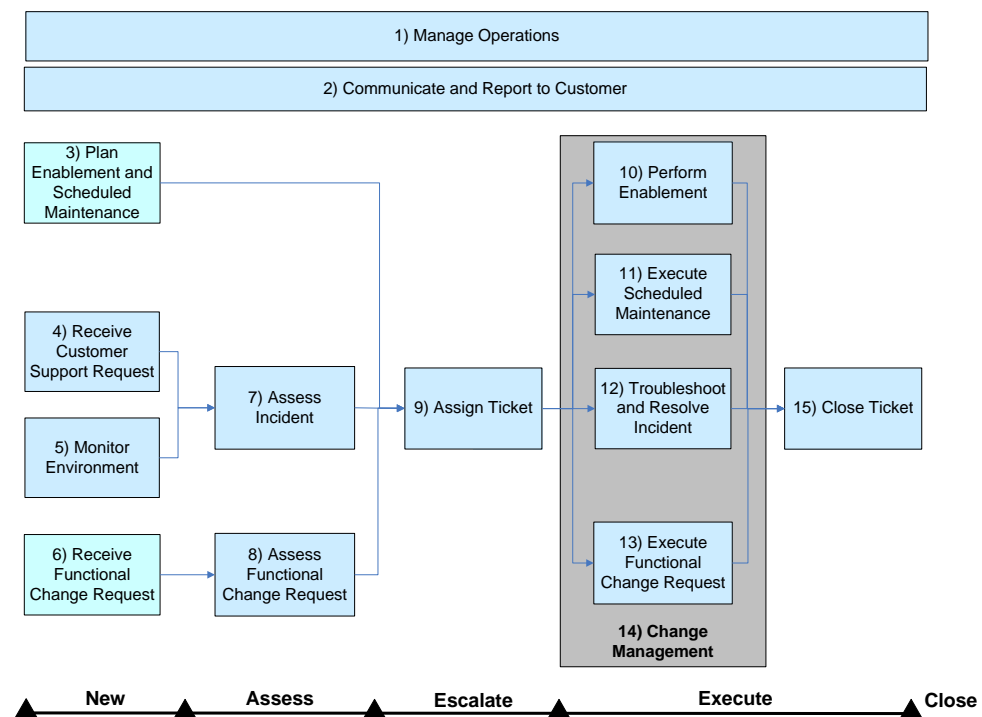


Figure No.5. NWN Incident Management Process Workflow.

- 1) **Activation and Notification Phase:** Incidents begin with the detection of an event.

- a) 24x7x365 Metrics and alarms – Monitoring and alarming of real time metrics and service dashboards. NCare utilizes early indicator alarms to proactively identify issues that may ultimately impact Customers.
  - b) Trouble ticket entered by an NCare employee.
  - c) 24X7X365 technical support hotline
- 2) **Recovery Phase** – Assigned Engineers will troubleshoot the incident. Once troubleshooting, break fix, and affected components are addressed, the call leader will assign next steps in terms of follow -up documentation and follow-up actions and end the call engagement.
- 3) **Reconstitution Phase** – Once the relevant fix activities are complete the call leader will declare that the recovery phase is complete. Post mortem and deep-root-cause analysis of the incident will occur. The results of the post mortem will be reviewed by relevant senior management and relevant actions will be documented and tracked to completion.

The Contract Manager described in Section 5 is accountable for ensuring all information is escalated to the appropriate individuals and is responsible for ensuring all contractual SLAs are documented. The Contract Manager is informed of all issue resolutions and root causes.

- 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.

**NWN Response:** NWN confirms that we will not engage in nor permit agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or Master Agreement. NWN requires all employees to comply with our standard security policy which explicitly prohibits the involvement of the development, transfer, or execution of malicious software. NWN employs industry best practice to block adware, malware, and other unwanted intrusions as is confirmed through our annual SSAE18 and CJIS audits/certifications.

NWN does not access or use Customer content for any purposes other than as legally required and to provide NWN services selected by each customer, to that customer and its end user. NWN never uses customer content or derives information from it for other purposes such as marketing or advertising.

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

**NWN Response:** As a Cloud Provider, NWN provides assessments, consulting, and tools (such as AWS CloudFormation) to implement testing, development, and staging environments. The customer requirements of the project will dictate in

which test/development environments are deployed and the actual design of which is the responsibility of the customer/purchasing entity.

NWN does have the full capacity to design, deploy, and manage test, develop and production environments as a Value Added Service.

- 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.

**NWN Response:** NWN certifies 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. NWN can offer VPAT information upon request as it depends upon solution.

- 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.

**NWN Response:** NWN confirms that our Cloud solutions are accessible using current versions of multiple browser platforms including Google Chrome, Mozilla Firefox, Microsoft Edge, and Microsoft Explorer.

- 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.

**NWN Response:** NWN confirms that prior to the execution of a Service Level Agreement, we will meet with the Purchasing Entity key stakeholders to identify sensitive or personal information that is subject to any law, rule or regulation providing for specific compliance obligations to be stored or used by NWN.

NWN Cloud process require/include regular NWN/Customer meetings and a Statement of Work (SOW). Every SOW requires clearly defined and mutually agreed upon Service Level Agreements (SLA). The NWN Project Manager (PM) has a Project Kickoff meeting with the customer's key stakeholders. The kickoff meeting includes a review of SLA's. Before starting any project, the PM requires signature of SOW (and therefore SLA's).

- 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.



**NWN Response:** NWN manages projects with a Documented and Proven Methodology that aligns with our customer's specific needs. Our project delivery methodology is consistent with the Project Management Institutes PMBOK guidelines. NWN will assign a project management resource (Project Manager) to manage all aspects of project delivery. The assigned Project Manager will leverage the NWN project methodology, to ensure the successful delivery of the project and will be in contact to coordinate project kickoff activities within two weeks of execution of SOW.

Please refer to Attachment No. 5. NWN Project Management Methodology to see our Project Management Methodology and Attachment No.6. NWN Project Provisioning Methodology for Process Documents

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.
- How Offeror will maintain discounts at the levels set forth in the contract.
- How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.
- How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.

**NWN Response:** With over two decades of successful and compliant contract management experience, NWN meets these requirements and commits to comply with these requirements. The Contract Management meets regularly with Participating Entity Contract Managers/Administrators to ensure compliance and acquire approvals as required.

The Contract Manager works with our Business Unit Product Managers and Contracting Entities (such as the State of Utah) to ensure below requirement are met by providing easy to read changes and holding face-to-face meeting either at their location or via web or video conferencing:

- Service Line Additions and Updates comply for RFP Requirements
- NWN maintains discount levels set forth in contract
- NWN reports to Purchasing Entities regarding changes in technology and work with them to recommend service updates that meet their needs
- NWN provides transition support to any Purchasing Entity whose operations may be negatively impacted by the service charge.

As needed, NWN will bring in subject matter experts from manufacturers to help explain any major changes or concerns.

#### 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;
- Escalation plan for addressing problems and/or complaints; and
- Service Level Agreement (SLA).

**NWN Response:** NWN manages projects with a Documented and Proven Methodology that aligns with our customer's specific needs. Our project delivery methodology follows industry best practice including those of Project Management Institute (MPI) as documented in the Project Management Book of Knowledge (PMBOK).

Our Dedicated Project Managers (PM) and documented Provisioning Processes that our technical and management performance is accurately reported and that SLA's are fully documented, analyzed, and reviewed with customer for any needed adjustment for improvements where applicable. The PM coordinates regular meetings that include documented status and follow up items as needed.

Our Dedicated Customer Delivery Manager (CDM) work closely with Dedicated PM during the Provisioning and OnBoarding Process for our Managed/Hosted Service to ensure a successful hand off. The CDM will provide weekly or monthly status or a determined by customer reports from transition throughout the life of the contract.

NWN's escalation process provides customers with the ability to resolve their issues promptly. The PM and CDM have the authority to resolve the issue promptly or escalate to management (up to executives as needed) to ensure that each customer issue is resolved. Please refer to Attachment No.7. NWN Customer Escalation Process for our detailed escalation plan.

**Quality Assurance:** NWN meets regularly with customers to review concerns, ideas for improvements, and specific issues. These meetings are documented and followed up with the customer through completion.

**SLA:** Please refer to Section 6. NWN Technical Response, Item 8.10 for NWN SLA.

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.



**NWN Response:** NWN currently assigns one lead representative for each entity executing a Participation Addendum and regularly connects with them to keep contact information current. NWN commits to maintain this requirement throughout RFP related contract.

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.

**NWN Response:** NWN's dedicated Technical Customer Service Reps are available 24x7x365. NWN commits to maintain this requirement throughout RFP related contract.

c. Customer Service Representative will respond to inquiries within one business day.

**NWN Response:** NWN's dedicated Customer Service Reps respond within 24 hours. NWN commits to maintain this requirement throughout RFP related contract.

d. You must provide design services for the applicable categories.

**NWN Response:** NWN offers design services for applicable categories. NWN commits to maintain this requirement throughout RFP related contract.

e. You must provide Installation Services for the applicable categories.

**NWN Response:** NWN offers Installation Services for applicable categories. NWN commits to maintain this requirement throughout RFP related contract.

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

**NWN Response:** NWN commits to ensuring that we protect customer's privacy and security. NWN follows NIST 800-53, protection of data requirements. NWN is CJIS and SSAE18 Certified confirming our commitment to hold, protect, and dispose of

data follow completion of any contract service; comply with all applicable laws and related to data privacy and security; and 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.

Security in the cloud is the responsibility of the Customer as the Customer retains control of what security they choose to implement to protect their own content, platform, applications, systems and networks similar to how they would for applications in their own on-site data center. More specifically, customer is solely responsible for configuring and managing security "in" the cloud.

- Customers continue to own their data.
- Customers choose the geographic location(s) in which to store their data—it does not move unless the customer decides to move it.
- Customers can download or delete their data whenever they like.
- Customers should consider the sensitivity of their data, and decide if and how to encrypt the data while it is in transit and at rest.

NWN is solely responsible for configuring and managing security "of" the cloud. Control responsibility is as follows:

- **Shared Responsibility:** Customer provides security and configurations of their software components – NWN provides security for its infrastructure.
- **Customer-Only Responsibility:** Customer is fully responsible for guest operating systems, deployed applications, and select networking resources (for example, firewalls).
- **NWN-Only Responsibility:** NWN manages the cloud infrastructure, including the network, data storage, system resources, data centers, physical security, reliability, and supporting hardware and software. NWN configures inherit features of applications that are built on top of the system.

NWN provides Value Added Services to assist Customers with assessing, designing, implementing, and operating secure environments.

**NWN's Privacy and Disclosure Policy:** Includes details on Types of information/data NWN collects, how NWN uses this data, and what data we share per laws and related requirements. All Customer Data Records are kept for minimum amount of time as required by Local, State, and Federal requirements prior to removal from NWN systems and transitioned or transferred to customer based on their requirements for transfer.

**NWN System Security Policy:** Addresses access control, auditing and use of hardware, operating systems, software, servers and backup requirements for all systems maintained and operated by NWN.

NWN Cloud Services are located in highly secure, reliable, and geographically redundant NWN core Data Centers. All devices are implemented in closed systems architecture, locally installed or within the NWN data center(s). Locally installed devices are secured by the customer. NWN logical security controls include application and network safeguards for the organization's systems including user ID and password access, authentication, access rights and authority levels. These measures were implemented to ensure that only authorized users are able to perform actions or access information in a network or workstation. The controls provided reasonable assurance that access to system resources (i.e., programs, data, tables, and parameters) is appropriate and restricted to properly authorized individuals.

NWN systems are protected with at least one of the following protection mechanisms: Biometric identification, passwords, a personal identification number (PIN), a callback procedure, or a token. Employee remote access to the NWN Managed Services systems are protected with two factor authentication: password and RSA token. All access into NWN from the Internet or other hostile networks, including external dial-up services are encrypted per the Network Security Policy. Customer data is protected by multiple layers of security including hardware based encryption and capable of hardware-based FIPS 140-2 compliant data encryption at rest. Customers can access self-service reporting by establishing a password-protected, encrypted session to the network monitoring portals located at NWN. Customers have permissions to view only their specific data.

NWN Cloud Services are provided as a service and provides customer management space. Infrastructure controls are specifically designed to compartmentalize customer data. Our secure infrastructure provides operating, monitoring, and managing the network and its elements. The environment has 3 distinct security zones:

- **Management Network:** A separate physical interface for connecting to network management systems.
- **Secure Environment:** Provide application and customer data storage, are firewall protected from the other networks, including the Internet, by IP Border Elements. Network traffic is load balanced, via redundant hardware, to provide workload distribution, increased performance, and automatic rerouting in the event of a communications or server failure.
- **Customer Network:** The majority, if not all, of the network components are in the NWN Cloud and not on the customer premises. Customers access the Cloud via an NWN data service, an NWN VPN, or via an Internet Service Provider (ISP) of their choice.

**Data Protection:** Customers retain ownership and control over their content and retain responsibilities relating to the security of that content as part of a “Shared Responsibility” model.

NWN manages security of the cloud with physical and logical control. NWN’s controls include Encryption and Cryptographic Mechanisms and NWN utilizes Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic. Application, service, or information system physically or logically separate user interface services from information storage and management services. NWN’s access to, use, and dissemination of data from restricted files are consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and NCIC Operating Manual.

NWN Services allows only the owner of any account data to access or manage them (password / role-based access). This includes creating, renaming, deleting and editing associated metadata. Customer data is never examined nor processed during normal procedures.

- **Role-based Privileges:** Each User ID and Password (for End-Users, Customer Administrators, NWN Customer Care, and NWN Network Management) is associated with a role that defines and restricts which privileges or rights are available to an individual user for accessing to communication channels and to data storage areas.
- **Data Storage Security:** NWN Services segregates stored data for each individual user.
- **Investigative Support:** NWN monitors all accesses and changes to its managed environment. Information is logged for auditing and troubleshooting purposes.

**Data Disposal:** NWN disposes of hardware and data when required due to hardware replacement, customer migration/removal or as requested by customer. Data and harddrive destruction are performed by preferred/certified onsite vendors through our Datacenter Support. All destruction is witnessed and verified by NWN personnel. NWN receives a certificate of destruction from the vendors detailing the items destroyed.

All software based Data removals from our systems are performed by certified NWN Personnel. They are responsible for tracking the deletion of any data in relation to customer request or customer removal through our incident and change management system.



**Converged Infrastructure Solution and Complementary Cloud Services:** Procedures (through AWS) include a decommissioning process that is

designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.



Our **NWNComm Collaboration Infrastructure Solution**: All devices are implemented in closed systems architecture, locally installed or within the NWNComm data center(s). Locally installed devices are secured by the customer and connected to a private MPLS network. Communications between one customer environments to another is not permitted other than through traditional PSTN connections or third-party video bridging services such as Cisco WebEx CMR. NWNComm Services does not examine the contents of conversations, which include voice, text, video, and file sharing. To further protect the transmission from unlawful interception, all conversations, chat conversations may be optionally encrypted and sent over secure communication channels using current networking standards.

## 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.
- 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.
- 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.
- 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).
- 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.

**NWN Response:** NWN has reviewed the RFP in full, including Attachment D – Scope of Services, and commit that our proposed solutions meet the Special Publication 800-145, applicable laws, Executive Orders, directives, policies, regulations,



standards, and any other relevant industry standard. NIST 800-145 is the definition of cloud computing with describing the following:

- **Essential Characteristics:** On Demand Self-Service, Broad Network Access, Resource Pooling, Rapid Elasticity, and Measured Service;
- **Service Models:** Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS);
- **Deployment Models:** Private Cloud, Public Cloud, or Hybrid Cloud;
- **Categorization of Risk:** Low or Medium

NWN has committed to its solutions complying with the NIST Framework as it relates to our NWN cloud services.

NWN is SSAE SOC 1/SOC2 (over 10 years) and CJIS version 5.3 Certified. Certifications available upon request. These Certification require a continuous commitment to maintain compliance. NWN adheres to HIPAA, PCI, NIST, and several other data compliance mandates for our regulated customer base.

Our certificates validate our commitment to Logical and Physical Security, Availability, Processing Integrity, Information Confidentiality, and Personal Information operational excellence. NWN invests and trains heavily on data security certification to ensure that our solutions are able to meet the rigorous data security and threat protection demands of customers who are in financial services, healthcare and other industries subject to stringent security and regulatory compliance such as HIPAA (Health Insurance Portability and Accountability Act), Sarbanes Oxley (SOX) and Payment Card industry (PCI), as well as internal business security requirements were critical. NWN regularly provides support for customer audits, and are audit-ready for customers requiring data security and threat protection compliance and certification.

In addition our Data Center Certifications are as follows:

- East Coast Data Center Certifications
  - SSAE-I6 SOC 3 Type III Certified
  - SSAE 18 Type 2 SOC 2
  - PCI-DSS1\*
  - GLBA and HIPAA standards annually.
  - ITAR and EU-US Privacy Shield registered
- West Coast Data Center Certifications
  - Energy Star
  - HIPAA
  - HITrust
  - PCI DSS
  - SSAE16
  - ISO 27001
  - Uptime Institute M&O Stamp of Approval

NWN Cloud systems are protected with at least one of the following protection mechanisms: Biometric identification, passwords, a personal identification number (PIN), a callback procedure, or a token. Employee remote access to the NWNComm managed services systems are protected with two factor authentication: password and RSA token. All access into NWN from the Internet or other hostile networks, including external dial-up services are encrypted per the Network Security Policy. Customer data is protected by multiple layers of security including hardware based encryption and capable of hardware-based FIPS 140-2 compliant data encryption at rest. Customers can access self-service reporting by establishing a password-protected, encrypted session to the network monitoring portals located at NWN. Customers have permissions to view only their specific data.

NWN's Cloud Services protect our customers business from external threats, including 24x7x365 log correlation monitoring to inspect traffic for potential threats (provided for firewalls, IDS & IPS) and 24x7x365 IT environment monitoring and scheduled maintenance to stay on top of existing and potential problems.



#### **Converged Infrastructure Solution and Complementary Cloud**

**Services:** The AWS network provides significant protection against traditional network security issues, and you can implement further protection. The following are a few examples:

- Distributed Denial of Service (DDoS) Attacks.
- Man in the Middle (MITM) Attacks.
- IP Spoofing.
- Port Scanning.
- Packet sniffing by other tenants

**NWN Security Services:** Include Intrusion Detection & Prevention, SEIM & Log Management, Network Access Control, Web Application Firewalling, and Data Loss Prevention.

**NWN Value Added Services:** Include Vulnerability and Penetrating Testing, Security and Risk Assessment, Regulatory Compliance Review, Business Impact Analysis, Security Policy Development, and Virtual CISO.

- 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.

**NWN Response:** NWN is SSAE SOC 1/SOC2 (over 10 years) and CJIS version 5.3 Certified. Certifications available upon request. These Certification require a continuous commitment to maintain compliance and specifies the requirements for

managing computer security incidents, including but not limited to, detecting, responding, investigating, monitoring, and logging. The following events shall be logged:

- Successful and unsuccessful system log-on attempts.
- Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
- Successful and unsuccessful attempts to change account passwords.
- Successful and unsuccessful actions by privileged accounts.
- Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.

Inspected evidence that successful/unsuccessful logon attempts to the network and systems are logged and retained for a minimum of three months. Inspected evidence that the security logs were periodically reviewed by appropriate personnel to identify suspicious activity.

Logs are maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log clearly identifies both the operator and the authorized receiving agency. III logs also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period. In addition to the use of purpose codes and logging information, all users must provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

In addition, our Intrusion Detection Tools and Techniques send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.

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

**NWN Response:** NWN complies with this requirement and restrict visibility of hosted Data and documents to specific users or groups. Customers can manage their user access and administrator level access.

- **Role-based Privileges:** Each User ID and Password (for End-Users, Customer Administrators, NWN Customer Care, and NWN Network Management) is associated with a role that defines and restricts which privileges or rights are available to an individual user for accessing to communication channels and to data storage areas.
- **Data Protection:** NWN Cloud Services allow only the owner of any account data to access or manage them (password/role-based access). This includes



creating, renaming, deleting and editing associated metadata. Customer data is never examined nor processed during normal procedures.

- **Data Storage Security:** Our Services segregate stored data for each individual user.

The information system displays an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system. The message, at a minimum, provides the following information:

- The user is accessing a restricted information system.
- System usage may be monitored, recorded, and subject to audit.
- Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
- Use of the system indicates consent to monitoring and recording.

- 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.

**NWN Response:** NWN complies with this requirement. In the event of a security incident *all customers impacted* are notified based on industry best practice standards for notification. NWN has processes and procedures in place to provide ongoing updates as an issue progresses and through resolution and post remediation to ensure any impact is documented and reviewed for process/architecture improvement. Notification timeframes are determined during the initial phases of engagement and documented in their contract and SLA documentation.

Our third party contracted security incident personnel ensure these communication requirements are met in a timely manner. The response to the incident or investigation may include:

- Incident Root Cause Analysis
- Incident Scope Analysis
- Forensic Analysis
- Keyword Searches
- Network Activity Monitoring
- Email Search and Correlation
- Remediation Recommendations

During which time impacted customers will receive appropriate and timely updates during each phase and resolution meeting state and federal standards and laws.

- 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.
- 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).

**NWN Response:** NWN complies with above requirements.



### Converged Infrastructure Solution and Complementary Cloud

**Services:** Our Converged Infrastructure solution leverages AWS' virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 3.2 published in April 2016.

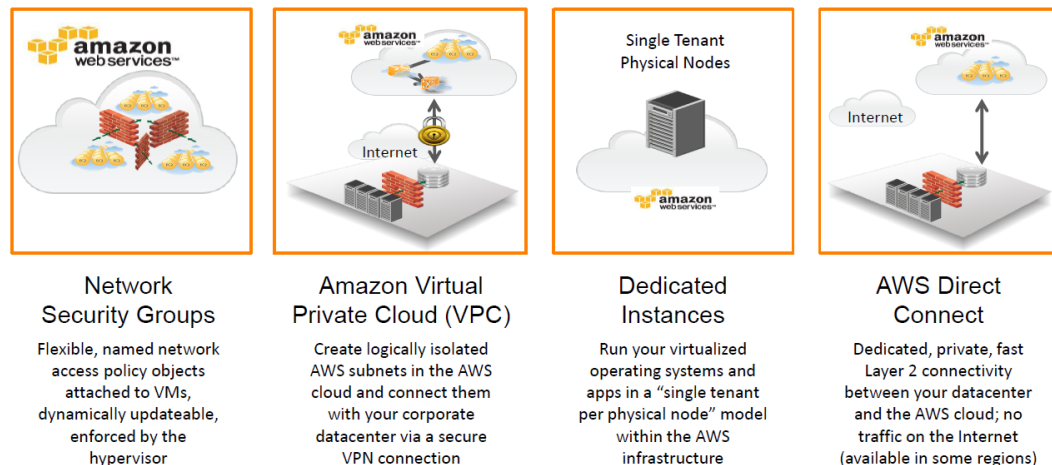


Figure No.6. AWS Architecture.



**Our NWNComm Collaboration Infrastructure Solution:** NWNComm leverages Cisco Virtualized MultiS erVICES Data Center (VMDC) for the data center architecture design. The VMDC system is the Cisco reference architecture for Infrastructure as a Service (IaaS) cloud deployments and utilizes a hierarchical network design for high availability and scalability.



The hierarchical or layered DC design uses redundant switches at each layer of the network topology for device-level failover that creates a highly available transport between end nodes using the network. DC networks often require additional services beyond basic packet forwarding, such as Server Load Balancing (SLB), firewall, and intrusion prevention. These services might be introduced as modules populating a slot of one of the switching nodes in the network or as standalone appliance devices. Each service approach also supports the deployment of redundant hardware to preserve high availability standards set by the network topology.

This layered approach is the basic foundation of the NWNComm Architecture to provide scalability, performance, flexibility, resiliency, and service assurance. VLANs and Virtual Routing and Forwarding (VRF) instances are used to provide customer isolation within the data center architecture, and routing protocols within the VRFs are utilized to interconnect the different networking and service devices.

Leveraging VMDC, the NWNComm architecture is built around the Cisco Unified Computing System (Cisco UCS), Nexus 1000V, Nexus 5000 and Nexus 7000 switches, multilayer Director Switch (MDS), Aggregation Services Router ASR 1000, Adaptive Security Appliance (ASA) 5585-X Nexus 1000V Virtual Security Gateway (VSG), VMware vSphere, and supports several shared storage options such as EMC and NetApp.

The following diagram shows the high-level architecture and components of the NWNComm solution.

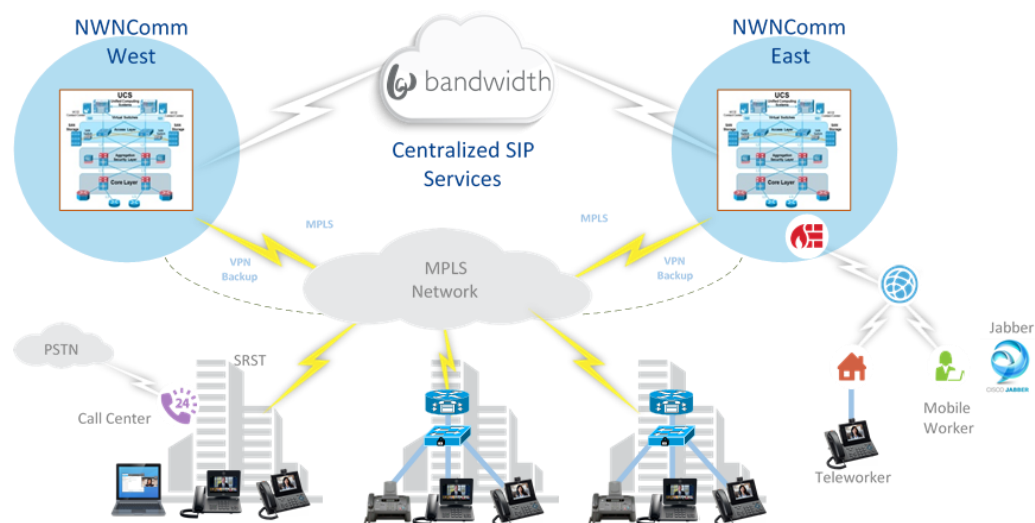


Figure No.7. NWNComm Architecture.

- 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.

**NWN Response:** NWN performs background checks of *all personnel* who have access to sensitive data prior to them gaining access to service areas and applications used to support clients. NWN Security Policies detail all background checks, access verifications, logging procedures etc. These procedures are verified by our third party auditors that verify these checks and procedures meet our SSAE and CJIS Certifications. All employees needing access to sensitive data and prior to them gaining access to service areas or applications are required to have a third party background check against the following standards.

- Criminal Background (National and Local)
- Sexual Offender
- Social Security
- Previous Employment
- Education Verification
- Credential

If further checks are required to meet more stringent needs, specific checks will be performed by NWN to meet those needs. NWN currently successfully require background checks for customers from Financial, HealthCare, Corrections and Rehabilitation Departments.

- 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.

**NWN Response:** Customer data is protected by multiple layers of security including hardware based encryption and capable of hardware-based FIPS 140-2 compliant data encryption at rest. Customers can access self-service reporting by establishing a password-protected, encrypted session to the network monitoring portals located at NWN. Customers have permissions to view only their specific data.

**Security of Confidential Data at Rest and In Transit:** Customers retain control and ownership of their data, and all data stored by NWN on behalf of customers has strong tenant isolation security and control capabilities. NWN offers the ability to add an additional layer of security to data at rest in the cloud by providing scalable and efficient encryption features.

NWN Services are provided as a service and provides customer management space. Infrastructure controls are specifically designed to compartmentalize customer data.

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.

**NWN Response:** All Incident management follows set standards and policies within NWN support infrastructure. Security incidents are handled by a designated team as described in our Security Policies which details assigned roles and responsibilities relating to these types of incidents. The incidents will follow the through the set of components, Tasks and Milestones described below with communications being provided at regular intervals as required through state and federal policies.

Component	Tasks	Milestones / Notes
<p>Acquire forensic data images of the suspected hard drive(s) and/or volatile memory to capture the current state and preserve evidence.</p> <p><i>(Note: Excludes disk imaging equipment fees where applicable (hard drives, cables, etc.)</i></p>	<ul style="list-style-type: none"> <li>Create a bit-level image of the hard drive and/or volatile memory for forensic evidence (performed onsite).</li> <li>Create a secondary copy of forensic evidence and supply to Security Vendor if required (performed onsite).</li> <li>Obtain all applicable log files from central audit sources.</li> </ul>	<ul style="list-style-type: none"> <li>Forensic data image(s) are created and retained by Vendor as part of analysis</li> <li>A copy of forensic data image(s) is supplied to vendor while onsite, sealed in tamper-evident packaging.</li> <li>Chain of Custody documentation is created and supplied while onsite.</li> </ul>
<p>Analyze the collected (imaged) data.</p>	<ul style="list-style-type: none"> <li>Perform off-line analysis on the suspect drives (performed offsite).</li> <li>Identify the amount and type of data present.</li> <li>Analyze the image for unusual files, such as attacker tools, misconfigurations, malware, and root kits.</li> <li>Review network, OS and application logs that may help determine the extent of the potential exposure.</li> </ul>	<ul style="list-style-type: none"> <li>Findings and recommendations will be included within the Incident Report.</li> <li>A list of data attributes identified on analyzed systems including any sensitive data elements.</li> </ul>

Identify the source of the compromise.	<ul style="list-style-type: none"> <li>• Make site visits to locations considered to be affected by the compromise.</li> <li>• Hold a debriefing meeting to understand the efforts that have taken place to date.</li> <li>• Conduct meeting with appropriate personnel to understand the network topology and data flow.</li> <li>• Document an Incident Report based upon applicable regulatory requirements.</li> </ul>	<ul style="list-style-type: none"> <li>• Create/compile network topology and data flow analysis documentation or diagrams.</li> <li>• Create Incident Report, including site visit report, findings and recommendations.</li> </ul>
Assess all network ingress / egress points within each in-scope physical location to be investigated.	<ul style="list-style-type: none"> <li>• catalog of all Internet IP addresses and/or phone numbers used for external connectivity.</li> <li>• Perform vulnerability assessment of each IP address.</li> <li>• Develop an external connectivity vulnerability report.</li> <li>• Deliver report for review.</li> </ul>	<ul style="list-style-type: none"> <li>• Create/compile External Vulnerability Assessment Report (included in final Incident Report).</li> </ul>
Vendor assumes the role of liaison/advisor for communications related to this incident between NWN and law enforcement or applicable third parties (e.g. regulators, public relations firms, etc.).	<ul style="list-style-type: none"> <li>• Attend conference calls and others to maintain communication and status.</li> <li>• Discuss efforts and findings.</li> <li>• Review any technical questions.</li> </ul>	<ul style="list-style-type: none"> <li>• Specific milestones detailed around communications and updates</li> </ul>
Perform log analysis to identify extent, duration, and impact of suspected incident.	<ul style="list-style-type: none"> <li>• Evaluate available log data to determine extent of compromise including, but not limited to, data attributes impacted, duration of incident, cause of incident, and impact on organization.</li> </ul>	<ul style="list-style-type: none"> <li>• Log analysis results will be documented in the final Incident Report.</li> </ul>



## 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.

**NWN Response:** NWN maintains services and SLAs during end of life closing down of a service and will maintain those through the contractual period. NWN customer configurations, CDR data and customer data are capable of being transferred securely if required to purchasing entities choice of location through secure electronic transfer or through secure carrier. NWN service specific configuration data is owned by NWN and considered proprietary data.

In the event that service to a Purchasing Entity will be closed down, the Purchasing Entity will define the close down requirements via a formal transition interview. During this communication, the Purchasing Entity will answer questions that will frame the close down process that will be meet their needs. The following will be identified:

- Data Transport
  - Will the data be exported for use by a subsequent provider
  - What format will best support the transition effort: XML, Excel, etc.
  - Will data export include only metadata (user lists, contracts, bill rates, etc.) or include historical data (timesheets for users, expenses for users, etc.).
- Data Protection
  - Will data remain in our data stores under standard security protocol until:
    - Conversion is complete
    - On continuous basis for historical access upon request by Purchasing Entity
    - Cutover Timing
  - What is the required access timeframe by Purchasing Entity identified personnel for accessing data after closed down What is the final date for time entry, invoicing, etc.

Closedown Process: Upon completion of the close down framework, the Product Service team will set contract end effective dates so that when the date is reached, all contracts in the system will be Ended and no further entries can be made. Subsequent to this, a full backup of data will be made and stored as requested by Purchasing Entity. Data cleansing will occur as directed by the Purchasing Entity and as required, will be maintained under standard security measures.

- 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.

**NWN Response:** Data can be transferred through secure encrypted data transfer or if required through physical secure carrier service in encrypted format. NWN maintains services and SLAs during end of life/closing down of a service and will maintain those through the contractual period. Negotiated return SLAs and caching times of data will be adhered to throughout the process as each contract can be adjusted to support timeframes and SLAs as customer requires.

## 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.
- Extended downtime.
  - Suffers an unrecoverable loss of data.
  - Offeror experiences a system failure.
  - Ability to recover and restore data within 4 business hours in the event of a severe system outage.
  - Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

### NWN Response:



**Converged Infrastructure Solution and Complementary Cloud Services:** NWN leverage AWS' Data center Business Continuity Management.

**Availability** - Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. Our solution provides the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers.

**Fault-Tolerant Design** - Our infrastructure has a high level of availability and provides the capability to deploy a resilient IT architecture. Our solution is designed



so systems tolerate system or hardware failures with minimal customer impact. Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

In addition to our solutions built in fault tolerance and high availability capabilities, NWN provides design and deployment services for AWS backup solutions utilizing N2WS Cloud Protection Manager. As a cloud-native backup tool built specifically for AWS, CloudProtection Manager gives your teams the ability to back up data as often as needed and recover it far more quickly than with traditional on-premises backup solutions, simplifying workloads and saving your teams time and resources. The ability to recover and restore data within 4 business hours in the event of a severe system outage would require a design and scoping engagement to develop a backup and restore solution to meet the 4 business hour window.



**NWNComm Collaboration Infrastructure Solution:** NWN's RPO and RTO is based on is fully GEO redundant with Active-Active Active-Failover Services across DCs. This highly available system provides for immediate recovery through active-active support cross datacenter. In the event of an actual restore of servers RPO is currently 30 second and RTO is 4 hour.

The NWN Cloud Architecture relies on a redundant pair of Data Center Interconnect (DCI) links to provide connectivity between the NWN East and NWN West Data Centers. These links are provider by different carriers for diversity and support up to 10GB of bandwidth each. Geo redundancy or high availability of a given data center requires infrastructure and applications running in multiple data centers to be available without any major down time. Several options are available to interconnect data centers in both active-active and active-standby deployment scenarios.

NWN uses an active-active data center deployment, where the applications are extended between data centers. Putting these nodes in separate data centers helps to build resilience into the cloud. This also provides the flexibility of being able to shift compute resources around geographically as needs dictate. NWN's active-active data center deployment is supported by Layer 3 Extension between Data Centers. Such extension provides routed connectivity between DCs used for segmentation, virtualization and the support of redundant applications.

Both datacenters are run in an active/active mode. NWN customers will have their redundant virtual servers in both data centers. The transport between NWN and the customer is also geo-redundant utilizing separate service providers for diversity.

Deploying two or more data centers in active-active mode allows NWN to provide scalable and highly available cloud services. The active data centers are in hot standby mode for each other.

Deploying applications at multiple active data centers is analogous to building a global server farm, which increases the number of requests and number of clients that can be handled. After content is distributed to multiple data centers, requests for distributed content must be managed. NWN manages the load by routing user requests for content to the appropriate data center. The selection of the appropriate data center can be based on server and application availability, content availability, network distance (proximity) from the client to the data center, and other parameters.

Level 3 geo-redundancy is offered in NWN deployments. As shown in the following figure, in normal operation Level 3 geo-redundancy includes the following:

- Two data centers with no real-time SAN mirroring.
- Data Center A has its management layer and publishers and subscribers backed up to a third-party site through SFTP daily.
- Load is shared between subscriber 1 and subscriber 2.

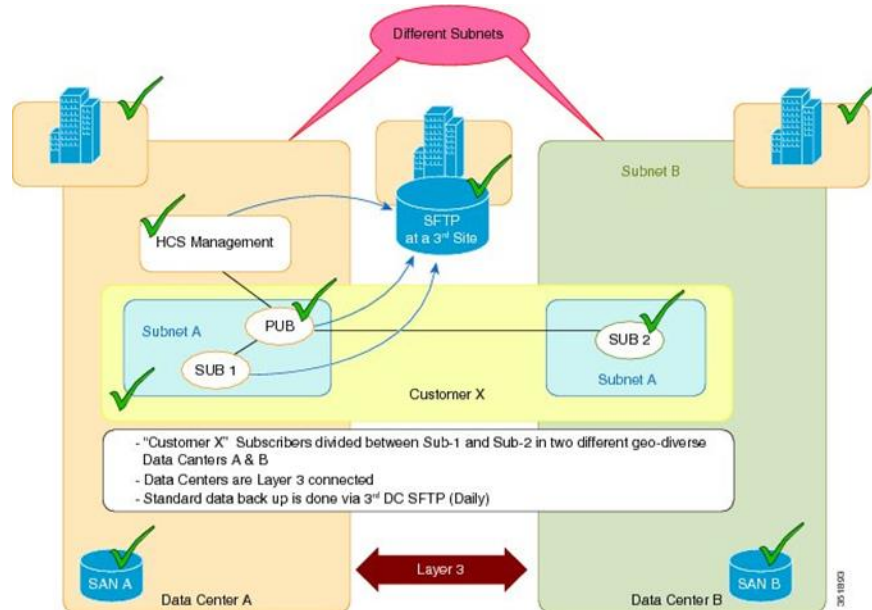


Figure No.8. NWNComm Level 3 Geo-redundancy

Unified Communications services offer many capabilities aimed at achieving high availability. They may be implemented in various ways, such as the following.

**Failover Redundancy:** For services that are considered essential, you should deploy redundant elements so that no single point of failure is present in the design.

The redundancy between the two (or more) elements is automated. For example, the clustering technology used in Cisco Unified Communications Manager allows for up to three servers to provide backup for each other. This type of redundancy may cross technological boundaries. For example, a phone may have as its first three preferred call control agents, three separate Unified Communications Manager servers belonging to the same call processing cluster. As a fourth choice, you can configure the phone to rely on a Cisco IOS router for call processing services.

**Redundant Links:** In some instances, it is advantageous to deploy redundant IP links, such as IP WAN links, to guard against the failure of a single WAN link.

**Geographical Diversity:** Some products support the distribution of redundant service nodes across WAN links so that, if an entire site is off-line (such as would be the case during an extended power outage exceeding the capabilities of provisioned UPS and generator backup systems), another site in a different location can ensure business continuance.

Within the NWNComm Architecture, all Unified Communications (UC) applications are deployed with application level redundancy to protect against any complete failure of a Unified Communications application. In addition, NWNComm deploys Unified Communications applications in a geo-redundant fashion, using well known techniques called clustering over the WAN.

- 8.8.2 Describe your methodologies for the following backup and restore services:
- a. Method of data backups
  - b. Method of server image backups
  - c. Digital location of backup storage (secondary storage, tape, etc.)
  - d. Alternate data center strategies for primary data centers within the continental United States.

**NWN Response:** A strict adherence to process and procedure ensures that customer data is fully protected. Customer data is replicated in near real time to remote geographically different datacenters. Replication occurs asynchronously with a defined 3-30 second protection window, which allows for recovery points to mirror this granular interval.

- **Method of Data and Server Image Backup:** Running workloads and service offerings are protected on a scheduled basis by using various protection policies including synthetic full backups and cumulative incremental to ensure the highest degree of protection without impact to the RPO and performance. Configuration changes, security events and troubleshooting logs are captured with these methods and retained for the duration of the SLA and customer requirements. Replication occurs

asynchronously with a defined 3-30 second protection window, which allows for recovery points to mirror this granular interval.

Method of Data Backup: Replication occurs at the storage level outside of the running workload so that performance is not impacted. Traffic traversing the data protection network is fully encrypted and when stored in the remote location, is managed by the data at rest encryption policies.

- **Digital Location:** Customer data is replicated in near real time to remote geographically different datacenters. Primary DataCenter is at our Raleigh North Carolina Location.
- **Alternate Location:** Our alternate is in Santa Clara California.

## 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.

**NWN Response:** NWN has several options for encrypting data at rest, ranging from automated AWS encryptions to other industry standard options including manual, customer-side options.

Customer data is protected by multiple layers of security including hardware based encryption and capable of hardware-based FIPS 140-2 compliant data encryption at rest. All access into NWN from the Internet or other hostile networks, including external dial-up services are encrypted per the Network Security Policy.

Our Cloud solution encrypts data using AES and FIPS 140-2 compliant encryption at rest. Encryption is used for implementation of cloud based services over a public based network occurs and when required to secure sensitive data based on the request and design of our customer's needs.

All access into NWN from the Internet or other hostile networks, including external dial-up services are encrypted per the Network Security Policy. NWN's controls include Encryption and Cryptographic Mechanisms and NWN utilizes Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic. Application, service, or information system physically or logically separate user interface services from information storage and management services.

NWN offers Services that provide support for both Internet Protocol Security (IPSec) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) for protection of data in transit.



### Converged Infrastructure Solution and Complementary Cloud

**Services:** NWN Converged Infrastructure Services offer several options for encrypting data at rest, ranging from completely automated AWS encryption solutions (such as AWS Key Management Service [KMS]) to manual, client-side options (such as AWS CloudHSM). Choosing the right solutions depends on which Cloud services are being used and customer requirements for key management.

- 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.

**NWN Response:** NWN complies with this requirement. We currently have BAA and other related agreements in place with multiple customers across the U.S.

- 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.

**NWN Response:** NWN commits to ensuring that we protect customer's privacy and security. NWN follows NIST 800-53, protection of data requirements. NWN is CJIS and SSAE18 Certified confirming our commitment to hold, protect, and dispose of data follow completion of any contract service; comply with all applicable laws and related to data privacy and security; and 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.

NWN confirms that we will not engage in nor permit agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or Master Agreement. NWN requires all employees to comply with our standard security policy which explicitly prohibits the involvement of the development, transfer, or execution of malicious software. NWN employs industry best practice to block adware, malware, and other unwanted intrusions as is confirmed through our annual SSAE18 and CJIS audits/certifications.

NWN does not access or use Customer content for any purposes other than as legally required and to provide NWN services selected by each customer, to that customer and its end user. NWN never uses customer content or derives information from it for other purposes such as marketing or advertising.



## 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.
- 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.

**NWN Response:** NWN offers the ability for Customers to negotiate Service Level Agreements (SLAs). NWN works with each customer to define the Statement of Work and in doing so review the SLA on a per project basis. SLA's are mutually agreed upon along with any required Key Performance Indicators. Service Levels will be calculated and reported monthly, and measured quarterly. Service Levels apply to support tasks based on priority and applicable NCare service.

However, NWN's SLAs are intended to ensure a common set of expectations between the Customer and NWN. Leveraging NWN standard SLAs provides more efficient communication, economies of scale, and solutions to issues.

NWN	Service Level Agreement
Service Availability	NWN services is available, measured from NWN's datacenter facility, 99.9% each month.[1]
MACD	Service Requests within NWN's control will be completed within the following timeframes (95%).[2], [3] <ul style="list-style-type: none"> <li>• Priority 1 = 4 hours</li> <li>• Priority 2 = 1 business day</li> <li>• Priority 3 = 2 business days</li> </ul>
Endpoint Add	Desktop phones, orders of no more than 5 units = 5 business days. [3]
Support Availability	NWNs Network Operations Center is staffed 7 X 24 X 365

[1] Excludes maintenance. Other components of service availability are architecture dependent.

[2] Requests that include a number greater than five is negotiated per customer as needed.

[3] Time for device procurement not included in this SLA.

A Sample of NWN NCare Managed Services SLAs with Priorities are defined:

Priority Level	Definition for Monitoring & Management Support Services
Priority 1	<ul style="list-style-type: none"> <li>A critical system or service is unavailable, causing a severe impact on operations. There is no alternative, redundant or back-up to this system or service.</li> </ul>
Priority 2	<ul style="list-style-type: none"> <li>A critical system or service is slowed or interrupted, however a work-around is in place so that operations can continue.</li> <li>A service interruption is occurring on a non-critical system or service.</li> </ul>
Priority 3	<ul style="list-style-type: none"> <li>The functionality of a non-critical system or service has been degraded.</li> <li>An error has been detected that is not affecting service performance or availability.</li> </ul>

Service	Service Level Agreement
<b>End User Helpdesk</b>	
Response: Speed of Answer	85% of calls will be answered within 60 seconds during support hours measured monthly across call queue <sup>[1]</sup>
Response: Abandonment	Less than 3% after 60 seconds
Response: Emailed case	Cases will be created in NWN's Case management system within 15 minutes of email arriving 85% of the time
Incident Resolution	<p>Incidents within NWN's control will be resolved within the following timeframes (80%).<sup>[2],[3]</sup></p> <ul style="list-style-type: none"> <li>Priority 1 – 4 hours</li> <li>Priority 2 – 1 business day</li> <li>Priority 3 – 2 business days</li> </ul>
Service Requests/MACDs	<p>Service Requests within NWN's control will be completed within the following timeframes (95%).<sup>[4],[5]</sup></p> <ul style="list-style-type: none"> <li>Priority 1 – 4 hours</li> <li>Priority 2 – 1 business day</li> </ul>



	<ul style="list-style-type: none"> <li>• Priority 3 – 2 business days</li> </ul>
Case management system	Online case management system will be available 7x24 (99.8%) excluding schedule maintenance.
<b>Network Operations Center (NOC)</b>	
Availability: Support Staff	NWN's Network Operations Center will be staffed 7 X 24 X 365
Response: Speed of Answer	90% of calls will be answered within 60 seconds.[6]
Response: Abandonment	Less than 3% after 60 seconds.[7]
Response: Email	Cases will be created in NWN's Case management system within 15 minutes of email arriving 95% of the time[8]
<b>Management Services</b>	
Incident support	<p>Incidents within NWN's control will be resolved within the following timeframes (80%).[9]</p> <ul style="list-style-type: none"> <li>• Priority 1 – 4 hours</li> <li>• Priority 2 – 2 business days</li> <li>• Priority 3 – 3 business days</li> </ul>
Scheduled maintenance	<p>Scheduled maintenance will be completed within the following timeframes (80%) after customer authorization.[10]</p> <ul style="list-style-type: none"> <li>• Priority 1 – 2 business days</li> <li>• Priority 2 – 5 business days</li> <li>• Priority 3 – 10 business days</li> </ul>
MACD's	<p>MACD's within NWN's control will be completed within the following timeframes (95%).[11].[12]</p> <ul style="list-style-type: none"> <li>• Priority 1 – 4 hours</li> <li>• Priority 2 – 1 business day</li> <li>• Priority 3 – 2 business days</li> </ul>
Functional change request	<p>Functional change requests completed within the following timeframes (80%) after customer authorization.[13]</p> <ul style="list-style-type: none"> <li>• Priority 1 – 2 business days</li> <li>• Priority 2 – 5 business days</li> <li>• Priority 3 – 10 business days</li> </ul>
<b>Monitoring Services</b>	
7x24 device monitoring and notification	Incidents will be identified within the following parameters (90%)[14]



	<ul style="list-style-type: none"> <li>• Priority 1 – 30 minutes</li> <li>• Priority 2 – 60 minutes</li> <li>• Priority 3 – 24 hours</li> </ul> <p>NWNs case tracking system will send confirmation of case creation via email within 1 hour 99%</p>
7x24 Online Monitoring Portal	Online monitoring portal available 7x24x365 (99.5%) excluding scheduled maintenance.
Monitoring	NWN will monitor devices 99.5% excluding schedule maintenance outages for monitoring system
<b>Reporting</b>	
Monthly reporting	Monthly reporting will be delivered within 10 business days of the end of the reporting period for services that include monthly reporting



**Converged Infrastructure Services – AWS Only:** Amazon Web Services SLAs are non-negotiable. Non-negotiable SLAs allow the Purchasing Entity to consume AWS resources at the optimal economies of scale. AWS provides [Service Level Agreements](#) (SLAs) that apply to customer use of specific services. Due to the rapidly evolving nature of AWS Cloud service offerings, our SLAs are best reviewed directly on our website via the links below:

- Amazon Compute SLA: <http://aws.amazon.com/ec2-sla/>
- Amazon Simple Storage Service (Amazon S3) SLA: <http://aws.amazon.com/s3-sla>
- Amazon CloudFront SLA: <http://aws.amazon.com/cloudfront/sla/>
- Amazon Route 53 SLA: <http://aws.amazon.com/route53/sla/>
- Amazon Relational Database Service (Amazon RDS) SLA: <http://aws.amazon.com/rds-sla/>
- AWS Shield Advanced SLA: <https://aws.amazon.com/shield/sla/>



#### NWNComm Collaboration Infrastructure Solution:

Priority Level	Definition
<b>MACD</b>	<p>Move, Add, Change or Deletion (MACD) process is intended for sites that are already deployed. MACD is related to the following:</p> <ul style="list-style-type: none"> <li>• Physical device or “soft” device (Jabber, IP Communicator)</li> <li>• End user (including voicemail PINs and passwords)</li> </ul>

	<ul style="list-style-type: none"> <li>Site based numbers (Extensions, Direct Inward Dial numbers and Auto Attendants).</li> <li>MACD SLA is for up to five users or end user devices and is intended for those sites that are already deployed</li> </ul>
<b>MACD - Move</b>	A programmatic relocation of a device, end user or number. Examples: <ul style="list-style-type: none"> <li>Move a phone from Location A to Location B</li> <li>Move an end user from Location A to Location B</li> <li>Move a DID or DN from Location A to Location B</li> </ul>
<b>MACD - Add</b>	A programmatic addition of a device, end user or number. Examples: <ul style="list-style-type: none"> <li>Add a phone and/or end user to Location</li> <li>Add Extension Mobility to an end user</li> <li>Add a VM box to an end user</li> </ul>
<b>MACD - Change</b>	A programmatic manipulation of existing configuration of a device, end user or number. Examples: <ul style="list-style-type: none"> <li>Change a phone model for an existing device</li> <li>Change a VM box PIN</li> <li>Change where an inbound DID or DN terminates</li> </ul>
<b>MACD - Delete</b>	A programmatic removal of existing configuration. Examples: <ul style="list-style-type: none"> <li>Delete a phone</li> <li>Delete an end user</li> <li>Delete a DID or DN</li> </ul>
<b>Priority 1 - MACD</b>	MACD involving a "VIP" (ex. Principal, Executive) or 911
<b>Priority 2 - MACD</b>	MACD involving a "Site/Location", inbound calls or multiple users (ex. Main Number, Hunt group, Auto Attendant, Contact Center number)
<b>Priority 3 - MACD</b>	All other Move, Add, Change or Deletions

### 8.11 (E) DATA DISPOSAL

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

**NWN Response:** NWN Data Disposal Policy follow existing best practices and meet the following industry standards as required.

- NIST 800-88
- HIPAA
- Sarbanes-Oxley Act
- Gramm-Leach-Bliley Act

- PCI Data Security Standard
- NSA/DoD Regulations
- NSA/CSS Regulations
- Identity Theft and Assumption Deterrence Act
- US Safe Harbor Provisions
- Bank Secrecy Act
- Patriot Act of 2002
- FDA Security Regulations
- Various state laws

NWN disposes of hardware and data when required due to hardware replacement, customer migration/removal or as requested by customer. Data and hard drive destruction are performed by preferred/certified onsite vendors through our Datacenter Support. All destruction is witnessed and verified by NWN personnel. NWN receives a certificate of destruction from the vendors detailing the items destroyed.

All software based Data removals from our systems are performed by certified NWN Personnel. They are responsible for tracking the deletion of any data in relation to customer request or customer removal through our incident and change management system.

All CDR data will be kept for minimum amount of time as required by Local, State, and Federal requirements prior to removal from NWN systems.

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

**NWN Response:** NWN meets the requirement of 99.5% and exceeds it with 99.9%. NWN currently provides large Cloud Customers with higher uptime to meet their unique needs.

NWN	Service Level Agreement
Service Availability	NWN services is available, measured from NWN's datacenter facility, 99.9% each month.[1]
MACD Service	Service Requests within NWN's control will be completed within the following timeframes (95%).2, 3 Priority 1 –4 hours Priority 2–1 business day Priority 3 –2 business days

Support Availability	NWNs Network Operations Center will be staffed 7 X 24 X 365
----------------------	---

NWN provides customers with options to extend the uptime of applications by providing a solution designed with fault tolerance using multiple availability zones, elastic load balancing, auto-scaling and regions.

- 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.

**NWN Response:** Each NWN Cloud service is supported by our Award Winning NCare team which provides 24x7x365 through our fully staffed Network Operations Center (NOC).

All incidents are created within NWN's ServiceNow ticketing system with real time notification delivery to customers. Customers can call NWN's 1-800 number, send an email to NOC team, or by using their own ServiceNow ticket system – depending on the customer needs.

Our NOC Team of Certified and Experienced Engineers provides the support and serves as the primary intake and initial triage and troubleshooting team for all Incidents. Engineering resources are available during hours as outlined in RFP as well as beyond in an on-call capacity.

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

**NWN Response:** SLA's are reported and reviewed on a monthly basis with the assigned Client Delivery Manager (CDM). Once reviewed, the CDM calculates any applicable credits and reviews those with the client. After credits have been agreed upon by both parties, the CDM submits to NWN's Finance Department for processing and to be recognized on the following months invoice.

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

**NWN Response:** All planned downtime follows our documented change control procedure. All maintenance changes follow our change management process and the customer is notified during normal and emergency system changes for approval and scheduling for least impact and risk.

A high-level summary of NWN's standard Change Management process is as follows:

1. Accept Request - NWN or the client completes the request. Assigned Solution Engineer accepts work.

2. Complete and Submit Change control request - Submit request for review by customer during regular change control meeting. Requests at a minimum should include:
  - a. Potential impact of change (from user perspective)
  - b. Detailed change procedure
  - c. Back-out plan if change is unsuccessful
  - d. Test plan to make sure environment is not impacted and change is complete
  - e. A proposed schedule and change control window for the change (during regular change windows set during enablement process unless change is an emergency)
3. Change Control Meeting for Customer Acceptance - A regular meeting is held to discuss active change controls. In this meeting the customer approves, approves with modification, or rejects the change control request. If rejected, the request may be reworked and sent back or discarded/cancelled.
4. Execute Change - Change is executed. If the change falls out of the approved window, it must be backed out unless the client explicitly extends the window.
5. Test - The change is tested for completion and for potential adverse impact to the environment and the users. Determination is made whether to back the change out.
6. Back Out Change - The change is backed-out as documented in the change control request.
7. Client Notification - The Client is notified of the results of the change.

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

**NWN Response:** SLA's are reported and reviewed on a monthly basis with the assigned Client Delivery Manager (CDM). Once reviewed, the CDM calculates any applicable credits and reviews those with the client. After credits have been agreed upon by both parties, the CDM submits to NWN's Finance Department for processing and to be recognized on the following months invoice.

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.

**NWN Response:** NWN provides Cloud Customers performance reports that are both real-time and/or batch statistics and are available over the Web.



**Converged Infrastructure Solution and Complementary Cloud**

**Services:** NWN Converged Infrastructure Cloud Services provides reporting that are captured in 1 or 5 minute increments depending on the customer's needs.



Figure No.9. NWNComm Level 3 Geo-redundancy



**NWNComm Collaboration Infrastructure Solution:** Our NWNComm solutions come with our own SmartComm. SmartComm is a complete suite to streamline the administration, improve support and monitor your NWNComm resources. This complete Suite provides a Provisioning, Administration and Self-care Portal (SmartComm Control) and a Reporting, Billing and Invoicing Portal (SmartComm Reporting).

SmartComm Control provides a Provisioning & Administration Portal for your support team while enabling a new "IT support" type experience for your end-users.



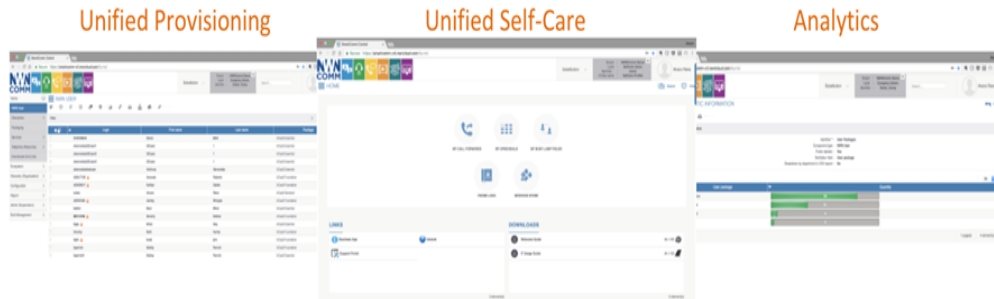


Figure No.10. SmartComm Managing Interface

SmartComm reporting streamlines and monitor your resources usage, volume and trends. Allowing you to monitor activity, spot fraudulent usage, distribute costs, legal inquiries and charge backs.



Figure No.11. SmartComm Reports

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

**NWN Response:** NWN Cloud Services meets this requirement and allows the ability to print historical, statistical, and usage reports locally.

8.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365. All onsite deployments are supported as part of our onsite engineering staff and can be scheduled to meet customer timing and needs.

**NWN Response:** NWN Cloud Services meets this requirement with on-demand 24x365 deployment.

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

**NWN Response:** NWN Cloud Services meets this requirement with ability to scale-up or scale-down 24x365 through our Self-Service Portal.

### 8.13 (E) CLOUD SECURITY ALLIANCE

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

- Completion of a CSA STAR Self-Assessment. (3 points)
- Completion of Exhibits 1 **and** 2 to Attachment B. (3 points)
- Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)
- Completion CSA STAR Continuous Monitoring. (5 points)

**NWN Response:** NWN Cloud Services meets this requirement and has completed CSA STAR Self-Assessment.

AWS meets this requirement and has completed CSA STAR Self-Assessment.

Please refer to Attachment No. 1. CSA STAR Registry for NWN's and AWS CSA STAR Self-Assessment.

### 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.

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

**NWN Response:** NWN Cloud Services meets this requirement.



#### **Converged Infrastructure Solution and Complementary Cloud**

**Services:** NWN Converged Infrastructure AWS Services offers Elastic Load Balancing and Auto Scaling that provide customers with the ability to automatically scale cloud-based resources up to meet unexpected demand, and then scale those resources down as demand decreases.



**NWNComm Collaboration Infrastructure Solution:** NWNComm services can be deployed in an emergency fashion with a preapproved purchase order and selection of services. NWN will follow the same methodology as answered in section 8.14.2 however with shorter installation timeframes for each phase of the project. In order to supply SIP connectivity requirements for existing internet connectivity at the site/s will be required, otherwise a buildout of circuit connectivity will need to



occur to our datacenters which ranges in time from 60 to 90 days depending on location and size.

### Sample NWNComm Project Milestones:

Start dates are from the SOW Effective Date.

Milestones	Description	Estimated Start Date
Initiate	Project Kickoff, Design & Planning	30 days
Assess	Data Collection and Analysis, Feature and Configuration Profiles, End User Requirements	30 days
Design	Design Sessions, Documentation, Integration Plan, Test Plan, Gateway Reviews & Signoffs	60 days
Prepare	Build the Initial Unit (Pilot)	90 days
Execute	Production Integrations/Migrations, Cut Over, and Train Users	120 days
Transition	Day 2 Support, Documentation, Transfer to Support	Upon completion of each Execution

*\*Please note that inaccurate Network, Telecom, Port, Device Count and/or Location (Number of Site Cuts) Information from Customer can create delays in the above schedule and/or require additional charges via a Change Request.*

## 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.

**NWN Response:** NWN meets this requirement and provides data retention periods based on customer needs, but minimums are based on State and Federal Standards and/or legal requirements .

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

**NWN Response:** Disaster recovery and backup are built into application environment and are available for in accordance to SLA. Inherent risks include additional costs, capacity planning, and replication failures but are minimized

through proper planning and utilizing redundant datacenters in Active-Active deployment.

NWN's GEO redundant active-active solution provides resolution of one site recovery or backup and restore functionality. All systems are backed up and mirrored to the opposite datacenter to ensure full disaster recovery across site if required. Both datacenters can provide full failover capabilities and functionality in the case of a regional disaster.

- 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.

**NWN Response:** Our multiple datacenters are within the United States and run in an active/active mode providing redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.



#### **Converged Infrastructure Solution and Complementary Cloud**

**Services:** NWN Converged Infrastructure AWS Services offers multiple data centers within the U.S. AWS Cloud infrastructure is built around regions and Availability Zones. A region is a physical location where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities. These Availability Zones offer customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible with a single data center.



**NWNComm Collaboration Infrastructure Solution:** The transport between NWNComm and the customer is also geo-redundant utilizing separate service providers for diversity. Deploying two or more data centers in active-active mode allows NWN to provide scalable and highly available cloud services.

The active data centers are in hot standby mode for each other. Deploying applications at multiple active data centers is analogous to building a server farm, which increases the number of requests and number of clients that can be handled. After content is distributed to multiple data centers, requests for distributed content must be managed. NWNComm manages the load by routing user requests for content to the appropriate data center. The selection of the appropriate data center can be based on server and application availability, content availability, network distance (proximity) from the client to the data center, and other parameters.

Level 3 geo-redundancy is offered in NWNComm deployments. As shown in the following figure, in normal operation Level 3 geo-redundancy includes the following:

- Two data centers with no real-time SAN mirroring.
- Data Center A has its management layer and publishers and subscribers backed up to a third-party site through SFTP daily.
- Load is shared between subscriber 1 and subscriber 2.

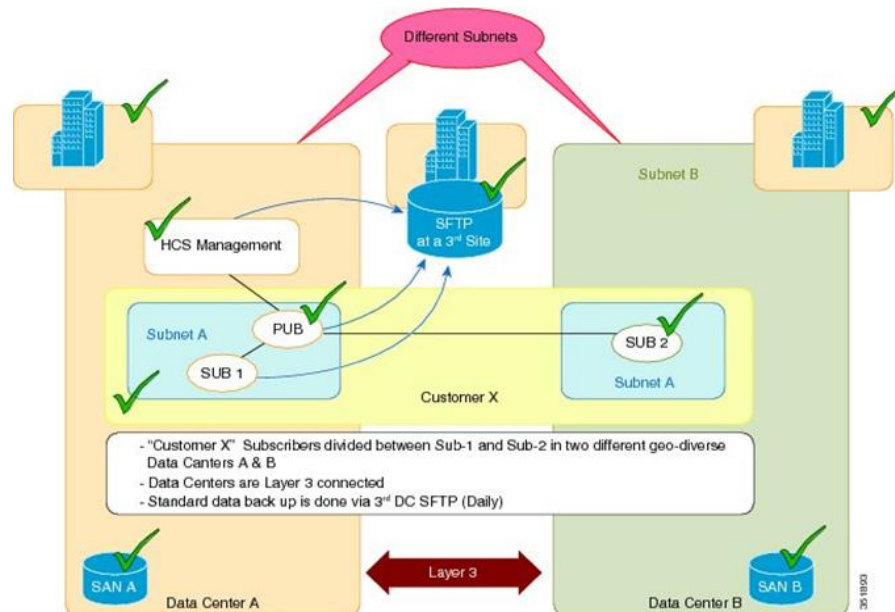


Figure No.12. NWNComm Level 3 Geo-redundancy

Unified Communications services offer many capabilities aimed at achieving high availability. They may be implemented in various ways, such as the following.

**Failover Redundancy:** For services that are considered essential, you should deploy redundant elements so that no single point of failure is present in the design. The redundancy between the two (or more) elements is automated. For example, the clustering technology used in Cisco Unified Communications Manager allows for up to three servers to provide backup for each other. This type of redundancy may cross technological boundaries. For example, a phone may have as its first three preferred call control agents, three separate Unified Communications Manager servers belonging to the same call processing cluster. As a fourth choice, you can configure the phone to rely on a Cisco IOS router for call processing services.

**Redundant Links:** In some instances, it is advantageous to deploy redundant IP links, such as IP WAN links, to guard against the failure of a single WAN link.

**Geographical Diversity:** Some products support the distribution of redundant service nodes across WAN links so that, if an entire site is off-line (such as would be the case during an extended power outage exceeding the capabilities of provisioned UPS and generator backup systems), another site in a different location can ensure business continuance.

Within the NWNComm Architecture, all Unified Communications (UC) applications are deployed with application level redundancy to protect against any complete failure of a Unified Communications application. In addition, NWNComm deploys Unified Communications applications in a geo-redundant fashion, using well known techniques called clustering over the WAN.

## 8.16 (E) HOSTING AND PROVISIONING

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

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.)
2. Creating and storing server images for future multiple deployments
3. Securing additional storage space
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).

**NWN Response:** NWN meets this requirement with a well-defined and documented process that optimizes deployments through a single portal.



### **Converged Infrastructure Solution and Complementary Cloud**

**Services:** NWN Converged Infrastructure AWS Services leverages AWS Management Console. Customers can use the AWS Management Console to perform any number of tasks, from deploying new applications to monitoring the health of applications. The AWS Management Console supports all AWS Regions and lets customers' provision resources across multiple regions.

AWS offerings are provided with a range of supporting components like management tools, networking services, and application augmentation services, with multiple interfaces to AWS Application Programming Interface (API)-based services, including Software Development Kits (SDKs), Integrated Development Environment (IDE) toolkits, and Command Line Tools:

<http://aws.amazon.com/tools/>.

**Management Tools** - AWS provides a broad set of services that help IT administrators, systems administrators, and developers more easily manage

and monitor their resources. Using these fully managed services, customers can automatically provision, configure, and manage their AWS or on-premises resources at scale.

**Resource Provisioning** - AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. Customers can use AWS CloudFormation's sample templates or create their own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run their application.



**NWNComm Collaboration Infrastructure Solution:** NWNComm provisioning stack is comprised of Microsoft, VMware, Cisco and Linux automation technologies which allows for seamless management and handoff between teams – Provisioning Team, Unified Communication Team, Datacenter Infrastructure Team and Monitoring Team. NWNComm leverages Cisco Virtualized MultiServices Data Center (VMDC) for the data center architecture design.

The VMDC system is the Cisco reference architecture for Infrastructure as a Service (IaaS) cloud deployments and utilizes a hierarchical network design for high availability and scalability. The hierarchical or layered DC design uses redundant switches at each layer of the network topology for device-level failover that creates a highly available transport between end nodes using the network. DC networks often require additional services beyond basic packet forwarding, such as Server Load Balancing (SLB), firewall, and intrusion prevention. These services might be introduced as modules populating a slot of one of the switching nodes in the network or as standalone appliance devices. Each service approach also supports the deployment of redundant hardware to preserve high availability standards set by the network topology. This layered approach is the basic foundation of the NWNComm Architecture to provide scalability, performance, flexibility, resiliency, and service assurance. VLANs and Virtual Routing and Forwarding (VRF) instances are used to provide customer isolation within the data center architecture, and routing protocols within the VRFs are utilized to interconnect the different networking and service devices.

Leveraging VMDC, the NWNComm architecture is built around the Cisco Unified Computing System (Cisco UCS), Nexus 1000V, Nexus 5000 and Nexus 7000 switches, multilayer Director Switch (MDS), Aggregation Services Router ASR 1000, Adaptive Security Appliance (ASA) 5585-X Nexus 1000V Virtual Security Gateway (VSG), VMware vSphere, and supports several shared storage options such as EMC and NetApp.

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

**NWN Response:** NWN provides a documented and proven process for trial and testing periods.

Testing, Pilots/Proof of Concepts, and Training are inherent in NWN's Statement of Work.

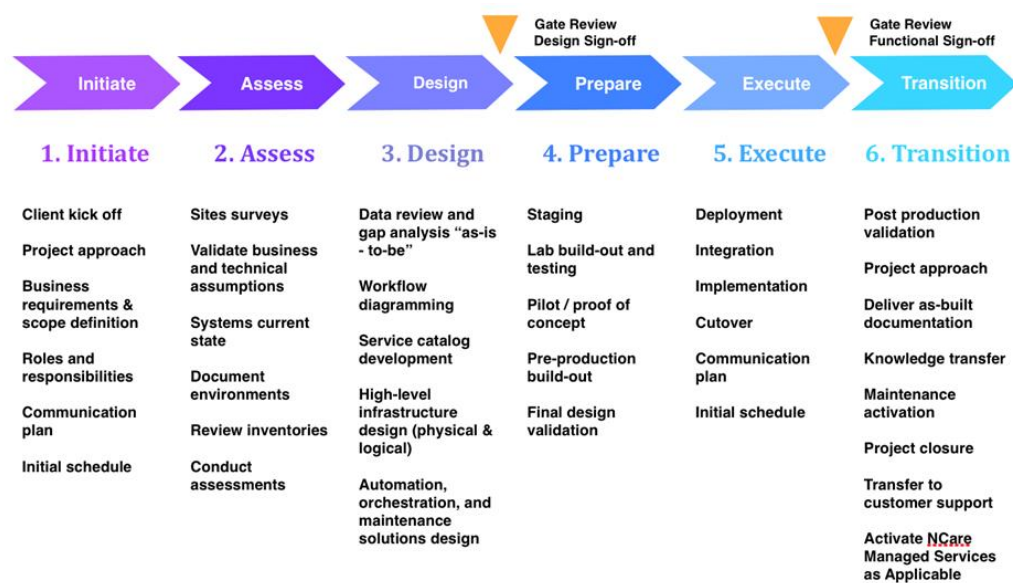


Figure No.13. NWN Provisioning Methodology.



### Converged Infrastructure Solution and Complementary Cloud

**Services:** NWN Converged Infrastructure AWS Services production systems may be easily cloned for use as development and test environments. Staging environments may be easily promoted to production.

The [AWS Developer Tools](#) help you securely store and version control your application's source code and automatically build, test, and deploy your application to AWS or your on-premises environment.



### NWNComm Collaboration Infrastructure Solution:

#### 1. Prepare Phase (Implementation and Testing)

- A. Provisioning
- B. Standard Phone Features - NWN will configure, test and label all station equipment including electronic sets, wall sets, and consoles (only if included with project). This shall include time during normal business hours for the rollout and testing of all station sets. The list below is a sample of the features NWN will configure. The final list of features and configurations are determined during the design phase.
- C. Existing Telephony Integrations
- 2. **Execute Phase (Cutover and Training)**
  - A. Phased implementation – NWN, working with the Customer’s technical team, will implement the new solution in phases as defined in the Design Phase (Pilot/Proof of Concept to limited implementation to larger implementations to complete implementation).
  - B. On Premise Equipment
  - C. Train the Trainer / End User Training - The training to be provided as part of this project in the form of “train the trainers” for which NWN will be responsible for:
    - Develop training plan and customize training material
    - Provide Customer with the training material in the form of Quick User Guides and/or Web Based Tutorial for future use.
  - D. Administration Training – NWN will provide training for each implementation. The exact type of training required will be determined during SOW negotiations.
  - E. Network/System Troubleshooting
  - F. GATE REVIEW: Production readiness acceptance
  - G. First Day in Service Support

Onsite engineering is now complete. Engineers will be focused on completing technical documentation, a review with the support team, and knowledge transfer. The Project Manager will verify approval for final billing, schedule and complete Project Review, and Closure meetings with Customer to acquire final Approval Signatures.

The project now enters into the Support and Management phase for the duration of the SOW.

## 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.

**NWN Response:** NWN invests heavily in our Engineers understanding of Technology and long-term relationships with our Cloud Partners. NWN Cloud

Services offer integrated solutions to other complementary applications and standard-interface to enable additional integrations.



### **Converged Infrastructure Solution and Complementary Cloud**

**Services:** NWN Converged Infrastructure Cloud Services provide a range of integration and compatibility capabilities. Cloud environments deployed on AWS can be treated as a logical extension of existing datacenters. Custom IP address space, Subnets, and VPN connectivity will enable customers to treat the AWS as a private connected datacenter to their infrastructure.

This means services on-premises can have network level integration to services running in AWS. Integration with AWS also means that customer's cloud server infrastructure can programmatically interact with other AWS services using published APIs. This infrastructure integration layer enables Auto-scaling, self-healing servers, automated capacity enhancements, and highly orchestrated services.



**NWNComm Collaboration Infrastructure Solution:** The NWNComm Solution has inherent integration capabilities with add-on services such as:

- Call Control Servers
- Voicemail with Unified Messaging Server(s)
- Instant Messaging Server(s)
- HCS-CC Server(s)
- Enhanced 911 Notification Server(s)
- Paging and Emergency Notification Server(s)/Gateway(s)
- Cisco ISR routers for PSTN connectivity

NWNComm offers the below features from key certified parts:

- **Voice and Video** – ISI and Verba Telemanagement Solutions, Verint Intelligence Solutions, Xmedius Fax Solutions, Cisco WebEx and Singlewire Emergency Mass Notification Systems;
- **Call Center** – Calabrio Workforce Management Suite and Zoom International WFO, Call and Video Recording for Call Centers, and Screen Capture.

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

**NWN Response:** NWN's Cloud Services and Solutions are customizable and personalizable to meet specific Purchasing Entities needs. NWN currently provides services for customers from small departments to large agencies and customers who have multiple locations (for example, throughout California).



Each cloud solution starts with the core offering and is able to be enhanced from a menu of options to support each of our unique customers' needs.

## 8.19 (E) MARKETING PLAN

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

**NWN Response:** NWN is pleased to present an offer to acquire a NASPO ValuePoint Contract and have been a heavy user of NASPO Contracts nationally for many years. We understand the importance of holding a NASPO contract and will leverage our proven Key Contract Marketing Plan that has supported NWN growth.

**Strategy:** Pair the power of AWS solutions with NWN's NWNComm and Value Added Services to the name of NASPO Cloud Contract to provide customers with a simple and well-known vehicle that makes procurement easy.

**Participating Entities:** Leverage our current and long-standing Participating Entity relationships to establish Participating Addendums across the U.S.

**Training:** NWN will hold regular internal training sessions with documented materials to our sales and business development managers to ensure that not only do they understand what solutions are available on the contract, but how to properly use the contract and the importance of compliance.

**WebSite:** Create a dedicated NWN NASPO Cloud Contract page that highlights the features and provides easy to use User Instructions. NWN Website: On a national basis, NWN maintains web pages that specifically focuses on our contracts and provides easy to use information, such as User Instructions, for our customers. Please see our webpages at [www.nwnit.com/contracts/overview](http://www.nwnit.com/contracts/overview).

**Events:** Incorporate what we learned during our National Marketing Events, where appropriate, to continually refine our message to what most benefits the audience. For Example:

- **Solution Based Events:** We have partnered closely with our key OEM Partners since the 1980's to market our NWN Solutions across the country with events that include Seminars, Webinar, Mailings, Interactive Trainings, etc.
- **Local Events:** that focus on K-12, Higher Education, Cities, and Counties: Promote our NASPO Cloud Contract to Local IT Leaders
- **Contract Focused Events:** Each of our offices across the county has had great success holding Annual Contracting Events where we partner with the State and our OEM Partners to present available solutions and easy to use User Instructions. Information also includes how to best leverage each contract to acquire those solutions. These events are regularly attended by State Agencies and Departments, Higher Education Entities, City and County Governments, as well as K-12 Entities. We work closely with the State Contracting Entities to ensure that our materials align to their needs.

**Drive Growth:** Our market penetration strategy starts from the top of the IT organization utilizing our deep relationships at the Executive level (CIO) and continue throughout the customers IT department to ensure that they have a

complete understanding of NWN's capabilities. We build brand awareness via aggressive marketing campaigns. Given our intimate knowledge of the offices market and our competitors, we will highlight how our depth of skills and broad experience with all offerings. As a result, we will differentiate ourselves from the competition and garner the visibility in IT organizations. As has always been our approach, we work with an organization's IT staff to provide seasoned technical infrastructure resources to assist them in understanding and developing solutions that will utilize best practices for their required projects.

**Collaboration:** NWN's Contract Manager and Marketing Team will interface with NASPO to continually redefine and improve our plan over the life of the contract. Our intent is to market our NASPO contracts nationally by highlighting available solutions.

**Partners:** NWN will continue to grow our NASPO business by executing a proven business plan that includes but not limited to:

- Partner Events that focus on current and new accounts to uncover new NASPO customers and opportunities.
- Direct Mail used for door opener campaigns.
- Seminars that focus on optimization and emerging Technology
- Tradeshows and Webinars that focus on Solutions and Training
- Online Marketing:
- Increased visibility on our website with videos, case studies, and SEO.
- Online advertising including on our NStore (eCommerce site).

## 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.

**NWN Response:** NWN is one of very few vendors that can provide AWS, NWNComm, and Workspace Cloud Solutions - all aligning to the RFP Cloud requirements. Along with a public sector focus – our Value Added Services are a key differentiator for NWN. Add in our decades of successful implementations and on-going support, our ability to provide the below Value Added Services is why global-leading OEM's come to NWN – such as Cisco to provide one of the first non-telecomm Hosted Collaboration Services and AWS to provide not only a face to our customers but the ability to manage AWS Cloud Services for our Customers.

### NWN Value Added Services:

- Cloud Readiness and Cloud Transition Assessments
- Security Assessments
- Cloud Infrastructure Consulting
- Infrastructure Planning and Design
- Cloud and Implementation and Integration Professional Services - offered on a Project Based (NPro) or on an "as needed" based (NWN Talent Acquisition Services)
- Award Winning 24x7 Management and Monitoring Services (NCare)

- Custom AWS Gold and Platinum Services.

Our Value Added Services allows our Customers IT staff to have confidence that they have the right solution that enables them to focus on their constituents and initiatives such as Digital Transformation and IoT Initiatives.

## 8.22 (E) SUPPORTING INFRASTRUCTURE

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

**NWN Response:** NWN Cloud Services vary on infrastructure needs.



### **Converged Infrastructure Solution and Complementary Cloud**

**Services:** NWN Converged Infrastructure Cloud Services do not require infrastructure to support any of our solutions as everything is provided via AWS. Entities can choose to use hardware based VPN services and on-premises Storage Gateway services if desired but this is not required. Additionally, customers may choose to have an AWS DirectConnect physical circuit between their environment and AWS.



**NWNComm Collaboration Infrastructure Solution:** NWNComm provides a majority of the infrastructure for the hosted solution in our data centers. NWN can support a high level of customization in which redundant hardware can be placed in the customer environment. As infrastructure required is dependent upon requirements NWN has outlined three areas in which infrastructure is needed:

**Solution Independent Infrastructure:** Below are a list of Infrastructure items that are required regardless of the solution, all of which can be deployed by NWN as a service:

- MPLS or VPN gateway to establish a secure connection to NWN
- LAN Switches capable of supporting a Voice VLAN and DHCP

**Optional Hybrid Solution Infrastructure:** Below are a list of infrastructure items that are optional based on customer requirements for premise based redundancy, all of which can be deployed by NWN as a service:

- Cisco C-Series Server(s) to host UC applications
- Cisco Voice Gateways to terminate local POTS or Telcom circuits

**Solution Dependent Infrastructure:** Below are a list of infrastructure items that will be deployed based on solution requirements, all of which can be deployed by NWN as a service:

- Analog Voice Gateways
- Power over Ethernet (PoE) Switches to power the IP Phones
- Cisco Voice Gateway(s) to interface with existing premise based system over T1/PRI
- Paging System Adaptor Modules

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

**NWN Response:** NWN is responsible for installation infrastructure specific to the cloud services procured and NWN incurs the cost.

NWN recommends that customers assess their cloud readiness and transition plan to ensure that their infrastructure, including backup and disaster recovery, before implementing any cloud solution to avoid unforeseen expenses and costs. NWN works with the customer to determine what their preference and skillset would be for the deployment of the infrastructure.

# Attachment No. 1. NWN CSA Star Registry

## Attachment No.1. CSA STAR Registry

### NWN CSA STAR Registry Self-Assessment

<https://cloudsecurityalliance.org/registry/nwn-corporation/>

<h3>NWN Corporation</h3> <p>NWN helps customers solve business problems with proven, relevant IT solutions and services. We keep pace with our customers' evolving technology needs, expanding our expertise into new and exciting solutions and applications. Our practical, cost effective solutions—from data center optimizati...</p>	<h3>Submission Info</h3> <p>Added: May 23rd, 2018</p>
<div style="display: flex; justify-content: space-around; margin-top: 20px;"> <div style="background-color: #f0e68c; padding: 5px 10px; border: 1px solid #ccc;">SELF-ASSESSMENT</div> <div style="background-color: #d3d3d3; padding: 5px 10px; border: 1px solid #ccc;">CERTIFICATION</div> <div style="background-color: #d3d3d3; padding: 5px 10px; border: 1px solid #ccc;">ATTESTATION</div> <div style="background-color: #d3d3d3; padding: 5px 10px; border: 1px solid #ccc;">C-STAR</div> <div style="background-color: #d3d3d3; padding: 5px 10px; border: 1px solid #ccc;">CONTINUOUS</div> </div>	

## Attachment No.1. CSA STAR Registry



Connect With Us: [in](#) [t](#) [f](#)

 [Search](#)

[BLOG](#) [MEMBERSHIP](#) [CERTIFICATION](#) [EDUCATION](#) [RESEARCH](#) [EVENTS](#) [CHAPTERS](#) [ABOUT](#)

Cloud Security Alliance > STAR Registry > STAR Registrant - NWN Corporation

### NWN Corporation

NWN helps customers solve business problems with proven, relevant IT solutions and services. We keep pace with our customers' evolving technology needs, expanding our expertise into new and exciting solutions and applications. Our practical, cost effective solutions—from data center optimization to cloud computing—are based upon your specific needs and environment, tailored to meet your business and financial objectives.

As a top partner for leading technology vendors, NWN has the resources and technology to empower your IT operation. With over 500 skilled employees, NWN offers the depth and knowledge of a large IT solutions provider, coupled with the personal service of a neighborhood firm. We take on your business challenge as our own and are accountable for smart, sensible IT solutions. We provide solutions we would choose for ourselves because they work.

**Added:** May 23rd, 2018

### NWNComm

NWN's NCloud platform features geo-redundant hosting to ensure high availability and minimal disruption to your day-to-day operations. We are dedicated to working as a team with you and your vendor-of-choice to architect a solution that best suits your needs. We also offer managed services to help you build, monitor and maintain your cloud implementation. NWN Comm is a cloud-based hosted communications platform, which includes voice, video, web conferencing, telecom, and contact center solutions. We integrate these essential capabilities with third party applications to create one easy-to-use and easy-to-manage solution.

STAR Self-Assessment

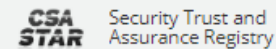
**Submitted:** May 23rd, 2018

Consensus Assessments Initiative Questionnaire v3.0.1

[Download](#)

#### Upcoming Meetings

No meetings currently posted. Check back soon.



STAR is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings.

- [STAR Information](#)
- [STAR Registry Entries](#)
- [STAR Submission Form](#)

#### Welcome New Members

The CSA is a member-driven organization, chartered with promoting the use of best practices for providing security assurance within Cloud Computing. We would like to welcome our newest members:

- [ST Engineering Electronics Ltd.](#)
- [IronOrbit](#)
- [GitHub](#)
- [HackerOne](#)
- [Digital Asset Custody Company, Inc](#)

[View all Members](#)




## Attachment No.1. CSA STAR Registry

### AWS CSA STAR Registry Self-Assessment

<https://cloudsecurityalliance.org/registry/amazon/>

## Amazon

Amazon Web Services provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world. With data center locations in the U.S., Europe, Brazil, Singapore, and Japan, customers across all industries ...



### Submission Info

Added: July 20th, 2012

[SELF-ASSESSMENT](#)
[CERTIFICATION](#)
[ATTESTATION](#)
[C-STAR](#)
[CONTINUOUS](#)



Connect With Us: [in](#) [twitter](#) [facebook](#)

Search ... [Search](#)

[BLOG](#) [MEMBERSHIP](#) [CERTIFICATION](#) [EDUCATION](#) [RESEARCH](#) [EVENTS](#) [CHAPTERS](#) [ABOUT](#)

Cloud Security Alliance > STAR Registry > STAR Registrant - Amazon

## Amazon

Amazon Web Services provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world. With data center locations in the U.S., Europe, Brazil, Singapore, and Japan, customers across all industries are taking advantage of the following benefits: Low Cost, Agility and Instant Elasticity, Open and Flexible and Secure.



Added: July 20th, 2012

### Amazon Web Services

STAR Self-Assessment

Submitted: January 19th, 2018

Consensus Assessments Initiative Questionnaire v3.0.1

[Download](#)

#### Upcoming Meetings

No meetings currently posted. Check back soon.



Security Trust and Assurance Registry

STAR is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings.

- [STAR Information](#)
- [STAR Registry Entries](#)
- [STAR Submission Form](#)



# Attachment No. 5. NWN Project Management Methodology



# Project Management Methodology

NWN manages projects with a documented and proven methodology that aligns with our customer's specific needs. Our project delivery methodology is consistent with the Project Management Institutes PMBOK guidelines.

NWN will assign a project management resource (Project Manager) to manage all aspects of project delivery. The assigned Project Manager will leverage the NWN project methodology, to ensure the successful delivery of the project and will be in contact to coordinate project kickoff activities within two weeks of execution of SOW.

## Assigned Project Manager

The following outlines the roles and responsibilities of the NWN Project Manager:

1. Act as a single point-of-contact
2. Conduct project kick-off activities and ensure thorough project communication with project stakeholders and team members
3. Schedule and facilitate weekly project status meetings with all relevant parties and stakeholders
4. Prepare, distribute & communicate weekly status reports, action item, opened and closed issues, critical paths and related project reports
5. Develop & maintain a detailed project plan, task plan, schedule & communications plan
6. Manage project scope and respond to change requests through the Project Change Request (PCR) process
7. Define and manage the escalation process
8. Review all project documentation and deliverables
9. Oversee knowledge transfer

In addition, a designated NWN Customer Enablement Manager will be assigned. Their role is to work hand-in-hand with your designated contacts as your advocate and to initiate activities that allow for a smooth transition from project activities to support activities.

## Assigned Enablement Project Manager

The following outlines the roles and responsibilities of the NWN Enablement Project Manager (CEM):

1. Customer advocate for any questions and concerns that may arise during project activities
2. Supports onboarding activities (establishing operating process, contacts for support)
3. Assures a smooth transition from integration/provisioning phases into the support phases of the project
4. Brings the customer relationship to a "steady-state" support phase



## Project Management Process

To deliver the highest quality project implementation, NWN brings a tightly controlled, comprehensive project management process that emphasizes detailed up-front discovery and design to help avoid costly, time-consuming missteps later in the deployment cycle. This approach has a proven track record of success.

## Major Milestones /Deliverables

Our documented and proven methodology includes:

- **Initiate** Project Kick Off meetings to review the scope with the project team and develop the project management plan
- **Assess** Current Target Infrastructure
- **Design**, Validate, Test and Pilot the New Environment
- **Prepare** Build the Initial Unit
- **Execute** Production Integrations/Migrations, Cut Over, and Train Users
- **Transition** your New Platform to Customer Support, Knowledge Transfer

## Project Work Breakdown Structure and Timeline

The Project work breakdown structure and timeline is planned and managed in Microsoft Project and is included in the Microsoft Project Task Plan.

## Requirements Management Process

The overall requirements management process is focused on handling the requirements after they have been initially approved. This includes maintaining changes or additions to the requirements throughout the entire project and tracking the requirements throughout the lifecycle.

## Roles and Responsibilities

Name	Risk Management Responsibilities
NWN Project Manager	Manages scope change requirements through leadership of the effort to communicate project requirements, document adjustments to project requirements and facilitates scope change management activities for all approved changes to requirements.
Project Team	Contributes to the identification of project requirements.

## Risk Management Process

The methodology utilized by NWN for risk management includes a progressive approach. As a project begins, many elements of the project are unknown. As the project progresses, more information is gained and project risks become more visible. Performing an initial Risk



Assessment will be the responsibility of the Project Manager. The Project Manager will determine the most appropriate method for executing the initial risk assessment. Identified Risks are tracked reviewed throughout project execution.

Funding for risk management is contained in the overall project budget. Changes in Scope due to risk mitigation activities will require change management.

## Roles and Responsibilities

Name	Risk Management Responsibilities
NWN Project Manager	Identifies project related risk, documents project risks, leads the effort to mitigate risk, and leads the effort to communicate project risk.
Project Team	Contributes to the identification of project risks. Assist in the mitigation of risks.

## Rules and Procedures

**Communication:** Communication regarding risk will follow the project communications plan.

**Tracking:** Tracking of risk elements and activities should be documented in the Risk Management Worksheet.

## Risk Impact Analysis Approach

The assigned Project Manager will utilize the initial Risk Assessment to determine the appropriate next steps in analyzing the project risk. The PM will document details regarding the project risks, the probability of occurrence, the anticipated impact to the project, the likely exposure and an agreed upon mitigation plan. Assigned Client Services Manager

At the beginning of your project, a dedicated NWN Client Services Manager is assigned. Their role is to manage the overall scope and to help you achieve the results you are looking for. The Client Services Manager coordinates the NWN team-- Professional Services, NCare Managed Services, Sales, Operations, and Finance organizations as well as works hand-in-hand with your designated contacts as your advocate for any questions and concerns that may arise during the project.

The following outlines the roles and responsibilities of the NWN Client Services Manager:

- A. Schedules monthly meetings which include the following:
  - Review SLA reports
  - Review all tickets that have been open and closed during a month
  - Review any tickets that remain open
  - Review changes to the “Customer’s” environment that may affect our service



- Review upcoming upgrades and new features/functionality they may provide
- Review upcoming scheduled maintenance or upgrades
- B. Manage new customer orders
- C. Program management of the contact between the “Customer” and NWN
- D. Manages the procurement of customer specific equipment and maintenance included in your solution
- E. Oversees implementation phases of the project
- F. Manages change orders and completion sign-offs
- G. Assures a smooth transition from the integration phases into the support phases of the project
- H. Manages customer relationship throughout implementation and support phases
- I. Provides overall program management responsibilities during steady state support.

## Change Management Process

The NWN Project Manager will utilize the Change Management Process to manage the lifecycle of all changes. All Change Requests will be documented, assigned and tracked for progress.

### Roles and Responsibilities

Name	Risk Management Responsibilities
NWN Project Manager	Documents project change requests, facilitate change request review and decision making, leads the effort to communicate change request and their status, escalates if change cannot be resolved by the review team and supports re-baselining activities if necessary
Project Team	Contributes to the identification of project risks. Assist in the mitigation of risks.

### Rules/Procedures

Any team member may submit a change request to the Project Manager. The requested change will be clearly documented and will explain any impact that the change will have on the project and associated deliverables. The project manager will review the request and determine if the change is appropriate. If so, it will be forwarded to the project sponsor for final decision.

### Change Impact Analysis Approach

Analysis of all requested changes will be performed to identify the impact of the change on the Project Costs, Risks, Schedule and Resources. The results of this analysis will be documented in the NWN Change Control Worksheet.

## Communications Management Process

Properly communicating on a project is a critical success factor for managing the expectations of all stakeholders. This includes reporting from the project team to the Project Manager and



reporting from the Project Manager to all stakeholders. The assigned Project Manager is the project communication steward for all project related information exchanges.

The sample Communications Matrix below provides an example of a project's communications. To keep the communications relevant and timely, we also include plans for collecting and responding to feedback.

Communication Item	Description / Purpose	Frequency	Audience
Project Kick-off Meeting	Meeting to describe a high level view of project, introduce project team members & their roles, communicate project structure & initial high-level business needs & setup future meetings	One-time	Customer, NWN
Project Team Status Meetings	Review project plan, progress & status, log & prioritize Constraints / Assumptions / Issues / Risks items, Critical Path (determine if any obstacles to completing critical tasks, escalate obstacles for resolution), share completed deliverables, discuss topics	Weekly throughout Implementation	Customer, NWN
Design Review Meetings	Team review of specification or technical design, satisfy that all issues are resolved & deliverable contents are complete	As Needed	Customer, NWN
Turnover Meetings	Formal handoff among NWN departments / disciplines	As Required	Project Stakeholders
Lessons Learned Meeting	Review opportunities for improvement & reinforcement of best practices	One-time	Project Stakeholders

## Time Management Plan

The time management plan must describe the process for controlling the proposed schedule and how the achievement of tasks and milestones will be identified and reported. The plan must also detail the process to identify, resolve, and report resolution of problems such as schedule slippage. The time management plan will include:

## Time Management Process

The NWN Project Manager is responsible for breaking down the implementation into measurable tasks and milestones. The work breakdown structure is applied to the project schedule and allows the Project Manager to closely monitor project timelines to avoid schedule overruns. Project Timeline health is reviewed in weekly status meetings to allow for timely identification of schedule slippage. If schedule slippage occurs, The Project Manager is



responsible for planning steps for resolution with the Project Team and communicating the plan and progress.

### **Role and Responsibilities**

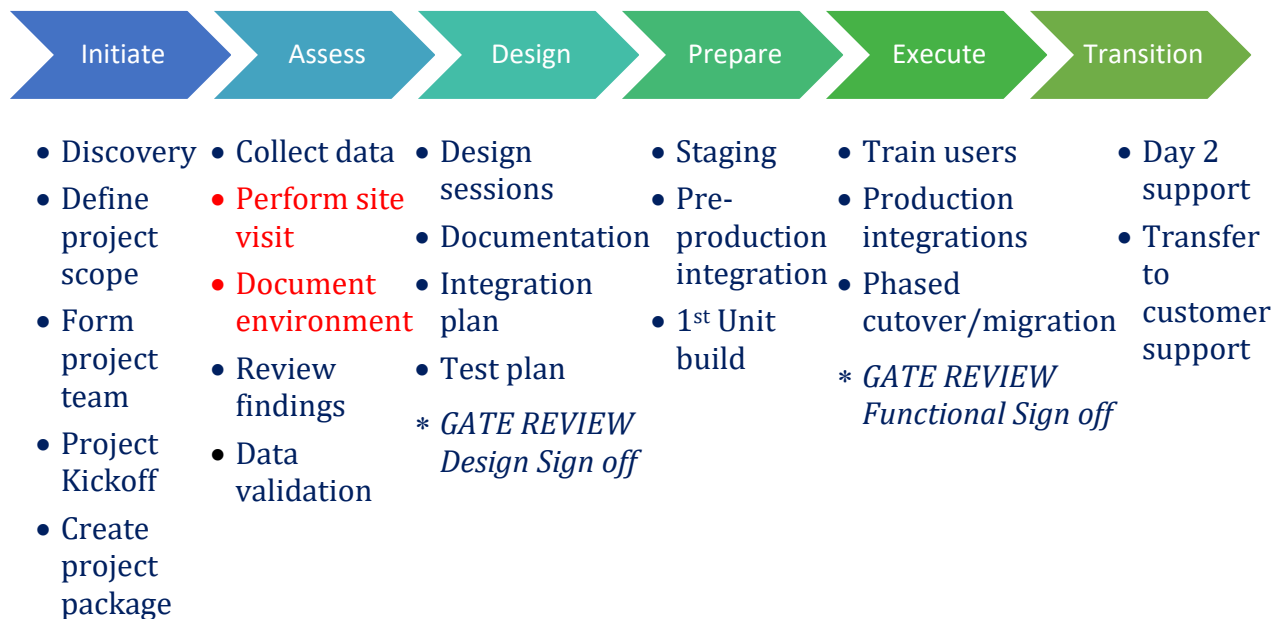
<b>Name</b>	<b>Risk Management Responsibilities</b>
NWN Project Manager	Responsible for Time Management during the implementation phase of the SOW.

# Attachment No.6. NWN Project Provisioning Methodology





# Project Provisioning Methodology



## Provisioning Process

### 1. Assess Phase

- A. Site visits – The NWN team will conduct site walk through sessions to collect data on the current environment and installation of the locations in scope. Site visit data collection includes: data rooms, communications closets, switch rooms, etc.  
(CALNET ONLY unless sold as part of project)
- B. Document Environmentals – NWN will compile a findings document and related recommendations based on the project scope and the site visit findings. This document will be presented and reviewed with Customer as the basis for the detailed design activities.  
(CALNET ONLY unless sold as part of project)
- C. End User Requirement Definition and Configuration Database Gathering – NWN will provide User Database form to be completed by the Customer and reviewed at the Design Meeting. These topics will include:
  - Coordinate with Customer to plan, design, and implement all station and telephone programmable features.
  - Perform Customer interview and key-sheet preparation/configuration database of end-user station requirements to be used for system programming and station deployment.
  - Create worksheets to guide Customer representatives to plan and design features such as line appearances, hunt groups, pick-up groups, etc.



- Port, Device Count and/or Location Information - Customer is to provide detailed, accurate, and current information to avoid delays in the above schedule which may require a Change Request correction.

**Milestones & Deliverables:**

1. Data Collection and Analysis
2. End User Requirement Definition

## 2. Design Phase

- A. Circuit design overview & planning – NWN will work with the Customer to integrate newly contracted circuits into the network topology. The Client will be included on communication and planning events including:
  - Scheduling and completion of vendor site survey
  - Installation of circuit
  - Extension of point of demarcation
  - Installation and testing of Out-of-Band access solution.
- B. Network Design Meeting (Delete for CALNET unless sold as part of project) – Review with Customer the network infrastructure requirements document and answer any Customer questions that have arisen. See Customer Expectations “Assumptions, Requirements, and Terms” section below.
- C. Design Meeting(s) – After the completion of the network design meetings, NWN and Customer’s team will hold a series of design meetings to discuss the technical aspects of the NWN Solution. NWN expects the Customer will come prepared with documentation and resources necessary to cover all topics. These topics will include:
  - Architecture and software version features review
  - Unified Communications device compatibility check
  - Migration strategies
  - User database review
  - Auto-Attendants and specialized voice-mail options
  - Call flows
  - Dial Plan
  - Discussion of downtime and risks
  - Customer responsibilities
  - Fax over IP current and future design
  - Integration into other systems
  - Application and voice gateway co-existence planning
  - End-user training requirements and training plan.
- D. Contact Center Design Meeting(s) – In addition to the NWNComm Design Meetings, NWN and the Contact Center stakeholders will meet to review and discuss the functional requirements for each of the individual Contact Center groups and the configuration of the new Contact Center System. NWN expects the Client will come prepared with documentation and resources necessary to cover all topics. These topics will include:
  - Contact Center groups operations and personnel



- Contact center call flows
  - Multi-channel strategy
  - Integration of 3rd-party applications (CRM, ERP, Ticketing System, Databases, etc.)
  - Discussion of downtime and risks
  - Historical and real-time (Live Data) reporting requirements
  - Prompts and greetings administration
  - Emergency call routing
  - Agent and Supervisor Training requirements and Training plan.
- E. Existing Telephony Integrations – NWN will work with Customer' IT staff to integrate the existing telephony solutions with NWN's hosted environment. A plan will be created that outlines system will co-exist in both environment (if possible) during the migration period.
- F. Vendor Communications – Once cutover strategy is defined, NWN and Customer will meet with NWN Contracted 3rd party vendors to establish, review and agree on cutover plan, if required. If other 3<sup>rd</sup> party vendors need to involved, then the Customer must coordinate the schedules for those vendors.
- G. "Fallback Plan" – NWN and Customer will build into the design a fallback plan for each stage of the migration. Being that the rollout will be a phased migration, dial plans and network connectivity will be in place for the migration, thus making a fallback plan easier to execute on.
- H. Gate Review – At the end of this Design meeting, NWN has gathered enough information to create final design document for the installation of the equipment. The design document will include configuration parameters specific to the install and any key technical decision made during design. The design will conform to Cisco guidelines and recommendations and the completed design document will be submitted for customer approval prior to proceeding with the install.

***Milestones & Deliverables:***

1. Design meeting and updated project plans for implementation of the Hosted Communications Solution.
2. Design Document(s) and Acceptance

### **3. Prepare Phase (Implementation and Testing)**

- A. Provisioning – NWN will provision the Solution which and all of its applications in NWN's Datacenter.

The NWN Solution will include the following components:

- Call Control Servers - These will provide call processing.
- Voicemail with Unified Messaging Server(s) – This will provide unified messaging services.
- Optional – Instant Messaging Server(s) – This will provide Instant Message and Presence
- Optional - HCS-CC Server(s) – This will provide contact center services.
- Optional - Enhanced 911 Notification Server(s) – This will provide E911 services.



- Optional – Paging and Emergency Notification Server(s) / Gateway(s) – this will provide paging services
  - Cisco ISR routers for PSTN connectivity – to be located in the customer Data Centers.
  - Establish MPLS Communication between Customer site(s) and Data Center.
  - NWN's service assurance, monitoring and management suite
- B. Standard Phone Features - NWN will configure, test and label all station equipment including electronic sets, wall sets, and consoles (only if included with project). This shall include time during normal business hours for the rollout and testing of all station sets. The list below is a sample of the features NWN will configure. The final list of features and configurations are determined during the design phase. The following is a sample of the features that will be implemented:
- Multiple line appearances on phone - Fast Transfer: Blind or Consult
  - Busy Lamp Field
  - Call Forward: <Busy, No Answer> Voicemail - Call Forward: <All> Restricted Access
  - Standard Ring-Tones
  - I-Divert active/inactive)
  - Call waiting (yes/no)
  - Internal Caller ID
  - External Caller ID (as supported by carrier) - Last Number Redial
  - Corporate Directory
  - Station Speed Dial with configuration changes from IP phone - Call Park
  - Meet-Me
  - Call Detail Records (enabled/disabled)
  - Out of "The Box" Music On Hold
  - Single Number Reach "Find Me, Follow Me"
  - As sited in Customer's Hosted VoIP Project.
- C. Existing Telephony Integrations – Implement integrations between the current telephony systems and NWN's hosted VoIP solution.

***Milestones & Deliverables:***

1. Provision Solution and Applications in NWN's Datacenter
2. Configure, Test and Label Station Equipment
3. Implement Integrations

**4. *Execute Phase (Cutover and Training)***

- A. Phased implementation – NWN, working with the Customer's technical team, will implement the new solution in phases as defined in the Design Phase
- B. On Premise Equipment – Below is a list of NWN owned equipment that will be placed on the Customer's premise.
- Add On-Premise equipment list if included in project.
- C. Train the Trainer / End User Training - The training to be provided as part of this project in the form of "train the trainers" for which NWN will be responsible for:
- Develop training plan and customize training material



- Provide Customer with the training material in the form of Quick User Guides and/or Web Based Tutorial for future use.
- D. Administration Training – NWN will provide training for each implementation. The exact type of training required will be determined during SOW negotiations.
- E. Network/System Troubleshooting – NWN will troubleshoot and diagnose technical issues associated with this project. Any issues that arise from Customer provided or owned devices and/or configurations related to the NWN Solution will require a change order and may affect the schedule of events planned for this project. NWN will work with Customer to isolate and identify network/system issues as well as provide assistance within reasonable boundaries. Any issues outside the scope of this project are the responsibility of Customer.
- F. GATE REVIEW: Production readiness acceptance – NWN will review the production cutover and implementation with the customer to verify that the solution is functioning in their environment as presented in this scope and the detailed design from the earlier Gate Review.
- G. First Day in Service Support – NWN will remain on site to help address and diagnose any problems that arise during the Unified Communications deployment within the scope of this project. NWN will troubleshoot configuration and integration issues arising from this project. NWN will review the production cutover and implementation with the customer to verify that the solution is functioning in their environment as presented in this scope and the detailed design from the earlier acceptance task. First Day Support does not include additional Moves, Adds, or Changes. NWN and the Client will formalize a detailed list of open items. Open items within the scope of this project will be addressed and resolved. Open items deferred due to Client availability will require a change order to complete.

***Milestones & Deliverables:***

1. Delivery of the detailed Bill of Materials (BOM) equipment &/or software components as identified in the Reference Materials section of this document.
2. Installation and Configuration of the NWN Solution based on parameters referenced in the approved Design Document:
3. Train the Trainer / End User Training
4. Solution Goes Live, Start Transition to Post Cut Over, Start of Invoice Date
5. First Day Support

**5. Transition (Transition to Post Cut Over Support)**

- A. Day 2 Support – NWN provisioning team remains on site to address and diagnose any problems that arise due to the migration to the new environment. NWN works with assigned persons as noted in “Assumptions and Requirements” section below to troubleshoot issues. Once the new system is agreed to be stable by NWN and Customer Designation Staff, NWN will start the process to finalize the documentation for the project.
- B. Knowledge Transfer – NWN’s technical team on the project conducts a solution orientation session and knowledge transfer with the Customer Designated Staff. This does not replace manufacturer specific technical training on the specific equipment, but provides a solid





overview of the final design and configuration and how to manage the environment using NWN's hosted collaboration administrative portal. Details of this session are:

- One session with up to four Customer staff at the Customer or NWN location.
- C. Transition Meeting to Support – NWN conducts a provisioning phase review, gains customer acceptance and transitions to the support phase of the SOW.

***Milestones & Deliverables:***

1. Project documentation, to include:
  - a. Project plan &/or task list
  - b. Action item list & Issues reports
  - c. Support 'Welcome Letter'

Onsite engineering is now complete. Engineers will be focused on completing technical documentation and a review with the support team. The Project Manager will verify approval for final billing, schedule and complete Project Review, and Closure meetings with Customer to acquire final Approval Signatures.

The project now enters into the Support and Management phase for the duration of the SOW.

## Support and Management Process (Post Cutover)

NWN will provide management of and support for the Solution. The Customer Enablement Manager will work with the assigned Customer Delivery Manager (CDM) to transition the responsibility for ensuring that NWN provides 24/7 system support services for the hosted solution.

The Customer may request support services by email or by calling the Network Operations Center. NWN will provide the customer with contact information as well as a list of description of who is authorized to open support cases with NWN.

NWN will assign a CDM to take ownership for all activities associated with the Customer account. Their role will be to manage the change request process, SLA Reporting, Customer communications and will act as the Customer's advocate.

### Assigned Customer Delivery Manager

The following outlines the roles and responsibilities of the NWN CDM:

- Schedules monthly meetings which include the following:
  - Review SLA reports
  - Review all tickets that have been open and closed during a month
  - Review any tickets that remain open
  - Review changes to the "Customer's" environment that may affect our service
  - Review upcoming upgrades and new features/functionality they may provide
  - Review upcoming scheduled maintenance or upgrades



- Manage new customer orders
- Program management of the contact between the “Customer” and NWN
- Manages change orders and completion sign-offs
- Manages customer relationship
- Provides overall program management

### Assigned Solution Engineer

A Solution Engineer is a level 2 engineer with a broad set of experiences. For all levels of support, a Solution Engineer is assigned to your environment to facilitate a deeper understanding of your environment to assist in troubleshooting issues. Also, they represent an additional point of contact into the managed services organization and a single point of escalation.

### Monitoring and Incident Support

NWN will monitor the health and performance of the NWN Solution and NWN-managed devices on Customer network. NWN will respond to alerts according to the Incident support information below. Examples of incidents NWN will resolve include:

- Communications Manager/Unity faults or hosted solution performance issues
- Gateway faults or performance issues
- Connectivity incidents or performance issues
- SIP or PRI Telco Connectivity
- User Administration (Moves, Adds, Changes and Deletes)
- RMA Processing (for covered devices)

Incidents are escalated based on Severity. Severity is defined in the below “Services Level Agreement” section. <<Insert State or RFP SLA as appropriate>>

Priority Level	Definition
Priority 1	<ul style="list-style-type: none"> <li>• A critical system or service is unavailable, causing a severe impact on operations. There is no alternative, redundant or back-up to this system or service.</li> </ul>
Priority 2	<ul style="list-style-type: none"> <li>• A critical system or service is slowed or interrupted, however a work-around is in place so that operations can continue.</li> <li>• A service interruption is occurring on a non-critical system or service.</li> </ul>
Priority 3	<ul style="list-style-type: none"> <li>• The functionality of a non-critical system or service has been degraded.</li> <li>• An error has been detected that is not affecting service performance or availability.</li> </ul>

- Should a Level 1 issue be identified, NWN will focus an engineer or team of engineers to fix the problem.





- Vendor escalation will, many times, be immediate. For Level 2 and Level 3 situations, the Customer and NWN will agree upon an action and escalation plan based upon criticality and resource availability.
- Customer will designate a list of authorized callers that NWN will validate for security purposes upon opening a new case. It is Customer's responsibility to notify NWN should this contact list change. Notifications should be emailed and all urgent changes should be followed up via a phone call to the NWN Command Center.
- For Customer-managed devices and applications that are part of the voice infrastructure (notably, switches & cabling), it is the Customer's responsibility to resolve incidents and to ensure compliance with individual vendor's requirements regarding version supportability. If NWN is asked to assist in troubleshooting Customer-managed devices and applications, additional hourly charges may apply.
- The Customer or desktop support partner will be responsible for physical movement, return, and replacement of handsets as well as providing appropriate switch connectivity and PoE for handsets.

## Monthly Management Reporting

Tracking and reporting are key components of the support services. On a monthly basis, NWN will provide a summary report of the work performed on the customer's behalf. This will include:

<<Insert State or RFP SLA as appropriate>>

1. Service Availability
2. Incident Management
3. MACDs
4. Change & Service Request Management

## Monthly Analysis reports

On a monthly basis, the Customer will receive an analysis report of NWN's performance against agreed upon Service Level Agreements (SLAs). NWN reviews monthly performance and YTD trending information.

## Notification Process <<Insert State or RFP SLA as appropriate or delete if not RFP>>

## Scheduled System Maintenance

NWN will perform maintenance on the Hosted Solution and supported client devices in order to keep the system healthy, backed up, and functioning optimally. Should a scheduled system maintenance activity result in system unavailability, NWN will perform that maintenance during an off-hours window and will provide a minimum of **1 week notice** to Customer's designated contacts.

NWN has industry standard defined and documented change windows. These windows are subject to change but can be reviewed with the customer at any time during the term of this SOW.



## **System Upgrades**

NWN will schedule to upgrade the Customer environment for Major Releases within 18 months of release. Allowances may be made for 3rd party applications that are integrated with the Customer environment. Customers will upgrade integrated Customer environments to compatibility to major OEM releases within 24 months.

NWN will upgrade Customer environments to Minor Releases upon agreement and as necessary.

## **Emergency System Maintenance (Un-scheduled)**

NWN reserves the right to perform emergency maintenance on the Hosted Solution and supported client devices in order to keep the system operational and functioning optimally. Should an emergency maintenance activity be required to either prevent or resolve an emergency, NWN will notify the appropriate customer contacts **as soon as possible** before actions are taken.

# Attachment No.7. NWN Customer Escalation Process

## NWN Customer Escalation Processes

NWN Corporation has successfully provided dedicated Contract Management Service Escalation support for over 30 years nationwide. NWN has the processes and infrastructure in place to support the State of Utah's needs. This methodology is based on the Worldwide Escalation Process (ITIL/itsm certified).

NWN has delivered over 1,000,000 products, for our other Public Sector contracts and have had less than thirty (30) instances the Help Desk or Contract Program Manager could not resolve. In those cases, once the issue/complaint was escalated to the next level, NWN personnel resolved ten within the next business day and the rest within five days. 100% of escalated issues have been solved locally and not been escalated beyond the local team. This process eliminates the time it takes to escalate an issue by having a local Contract Program Manager empowered to resolve issues.

NWN offers several managed services to our clients. Different services and service levels are entitled to different features and benefits. Some of our services are sold individually and others are packaged together to form a single comprehensive management solution.

### End-User Process for Escalating Service Request Issues

The end-user process for escalating service requests within a Customer's organization is to first contact the NWN Service Center. Once the end-user contacts the NWN Support Desk, NWN Engineers will be allocated and work to address case specific issue, and will escalate the issue to the next level support as appropriate if necessary. If at any time, the end-user is not satisfied with the progress being made to address the issue, he/she can call the next individual identified as part of the complaint escalation path, and so on up to the individual at the top of the path.

The NWN Service Center is responsible for problem resolution, Customer Satisfaction, contract deliverables, service-level attainment, and communication to the State and the NASPO CPM as necessary. The NASPO CPM will participate in reviews with the NOC to discuss any concerns and determine any additional services or changes that may be needed to maintain and improve satisfaction over the life of the contract.

Under normal operating circumstances, if an issue is not resolved at Level 1 within four hours, the Service Center will escalate the issue to the Level 2 support, the Assigned Solution Engineer (ASE) & Backup Assigned Engineer (BASE) (to be assigned per customer, upon engagement). At this point, the ASE or BASE will work to resolve the issue. *In rare cases where the ASE or BASE cannot resolve the issue at hand immediately, he will escalate the issue to our Level 3 support – CPM.* At this point, the CPM (with the assistance of the ASE or BASE) will work diligently to resolve the issue within the next business day. In the rare event that the issue is not resolved at this level, additional resources from within NWN will be allocated, by the CPM to resolve the outstanding issue.

### End-User Customer Service Support Team

An account team has been formed at NWN to work together on your behalf. These are people who will have more specific knowledge of your support agreement and your account.

NWN Service Center	The on-duty engineer in the Service Center is the always the first point of contact in directing questions or reporting issues to NWN.
Assigned Solutions Engineer (ASE)	The ASE will be introduced early to your account and will gain the most detailed knowledge of your environment.
Backup Assigned Solutions Engineer (BASE)	The BASE will handle incidents when the ASE is unavailable.
Contract Program Manager (CPM)	At any point if you feel that a particular problem or issue is not being dealt with in an appropriate manner you are encouraged to contact the NASPO CPM. The CPM will be able to discuss your concerns and find a solution rapidly.

Title	Name	Phone	Email
NWN Service Center	On-Duty Engineer	855-548-2200	support@nwnit.com
Assigned Solutions Engineer	TBA	TBA	TBA
Backup ASE	TBA	TBA	TBA
Contract Program Manager	TBA	TBA	TBA

***TBA – To Be Assigned – Once NWN has engaged an agency under the NASPO Contract, an ASE and BASE will be assigned to their account and contact information will be provided.***

## Calling the NWN Network Operations Center

Please follow the below procedure when calling the Service Center. This will help ensure that you spend the minimum amount of time on the phone and that we can start working your problem with as many of the facts in front of us as possible

- ✓ **If you have a question or an incident: Call the Service Center at 855-548-2200 or email [support@nwnit.com](mailto:support@nwnit.com)**
- ✓ **If you want to make a change to a monitored device or to named contacts, email [change@nwnit.com](mailto:change@nwnit.com)**

Only named assigned contacts should call or email the Service Center. This ensures that only persons authorized by your organization are cleared to open calls with NWN and it helps to manage call volumes.

The duty engineer will request (or please include in the email) the following information:

1. Your name
2. Company name
3. Phone number for call-back
4. Device name if applicable
5. Problem description or information request
6. Severity of incident

✓ **You will be assigned a ticket number**

At the time your call is entered into the ticketing system, you will be assigned a ticket number. All the details of the ticket are recorded for reference at NWN and to assist in the quickest resolution to problems. Ticket numbers are helpful when:

1. Checking the status of your ticket
2. Informing a duty engineer of additional information at a later date
3. Reporting on ticket history
4. Closing your incident

✓ **Your call will be assigned a priority**

**Priority 1:** A critical system or service is unavailable.

**Priority 2:** An issue has been detected where functionality is interrupted however there is either a work-around or the service interruption is occurring on a non-critical system or service.

**Priority 3:** The functionality of a non-critical system or service has been affected. An error has been detected that is easily corrected or is identified as a non-reoccurring or spurious.

✓ **Your call may be escalated**

When necessary, the Service Center engineer may contact your Assigned Solutions Engineer (ASE), Backup ASE, or one of NWN's many vendor-partners for assistance. Escalations are managed by priority.

**Priority 1:** The Service Center will escalate to your ASE or backup ASE via a warm hand-off. If the ASE is unavailable, the Network Operations Center will escalate to the backup ASE. Should the ASE and BASE both be unavailable, the Service Center will escalate internally to find an available engineer to begin troubleshooting immediately.

**Priority 2:** The Service Center will escalate your case to your ASE through NWN's ticketing system. Your ASE will respond to your request within one business day.

**Priority 3:** The Service Center will escalate your case to your ASE through NWN's ticketing system. Your ASE will respond to your request within three business days.

## **Our call escalation process for Priority 1 issues:**

When necessary, the Service Center engineer will escalate your issue via our established Priority 1 call process below:

1. **ASE** – the Service Center will contact the ASE for a warm hand-off
2. **BASE** – if ASE is unavailable, the Service Center will contact the BASE
3. **Team Lead** – If both the ASE and BASE are unavailable, the issue will be escalated to the Team Lead for resource allocation or resolution.
4. **CPM** – if ASE, BASE and Team Lead are unavailable, the issue will be escalated to the Contract Program Manager for resource allocation.
5. **Director of Customer Delivery** – if calls to ASE, BASE, Team Lead and CPM are unsuccessful, the Service Center will contact the Director of Customer Delivery for resource allocation to address the issue.
6. **VP of Service Delivery, NCare Managed Services** – if calls to all other parties have been unsuccessful, the Vice President for Service Delivery is contacted for assistance in resource allocation for the issue.
7. **Senior Vice President, NCare Managed Services** - if calls to all other parties have been unsuccessful, the Senior Vice President for Service Delivery is contacted for assistance in resource allocation for the issue.



**Attachment E – Service Offering EULAs, SLAs**

None at this time.