REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES FORM

By signing this Request for Proposal for Contractual Services form, the bidder guarantees compliance

CONTRACTOR MUST COMPLETE THE FOLLOWING

with the procedures stated in this Solicitation, and agrees to the terms and conditions unless otherwise indicated in writing and certifies that bidder maintains a drug free work place.

Per Nebraska's Transparency in Government Procurement Act, Neb. Rev Stat § 73-603 DAS is required to collect statistical information regarding the number of contracts awarded to Nebraska Contractors. This information is for statistical purposes only and will not be considered for contract award purposes.

_____ NEBRASKA CONTRACTOR AFFIDAVIT: Bidder hereby attests that bidder is a Nebraska Contractor. "Nebraska Contractor" shall mean any bidder who has maintained a bona fide place of business and at least one employee within this state for at least the six (6) months immediately preceding the posting date of this Solicitation.

_____ I hereby certify that I am a Resident disabled veteran or business located in a designated enterprise zone in accordance with Neb. Rev. Stat. § 73-107 and wish to have preference, if applicable, considered in the award of this contract.

_____ I hereby certify that I am a blind person licensed by the Commission for the Blind & Visually Impaired in accordance with Neb. Rev. Stat. §71-8611 and wish to have preference considered in the award of this contract.

FORM MUST BE SIGNED USING AN INDELIBLE METHOD OR BY DOCUSIGN

FIRM:	**NGA 911, LLC**
COMPLETE ADDRESS:	**8383 Wilshire Blvd, Ste 800, Beverly Hills, CO 90211**
TELEPHONE NUMBER:	**(916) 862-3373**
FAX NUMBER:	**(818) 487-1464**
DATE:	**5/28/2020**
SIGNATURE:	Michelle Bland
TYPED NAME & TITLE OF SIGNER:	**Senior Vice President, Operations**

II. TERMS AND CONDITIONS

Bidders should complete Sections II through VI as part of their proposal. Bidders should read the Terms and Conditions and should initial either accept, reject, or reject and provide alternative language for each clause. The bidder should also provide an explanation of why the bidder rejected the clause or rejected the clause and provided alternate language. By signing the solicitation, bidder is agreeing to be legally bound by all the accepted terms and conditions, and any proposed alternative terms and conditions submitted with the proposal. The State reserves the right to negotiate rejected or proposed alternative language. If the State and bidder fail to agree on the final Terms and Conditions, the State reserves the right to reject the proposal. The State of Nebraska is soliciting proposals in response to this solicitation. The State of Nebraska reserves the right to reject proposals that attempt to substitute the bidder's commercial contracts and/or documents for this solicitation.

Bidders should submit with their proposal any license, user agreement, service level agreement, or similar documents that the bidder wants incorporated in the Contract. The State will not consider incorporation of any document not submitted with the bidder's proposal as the document will not have been included in the evaluation process. These documents shall be subject to negotiation and will be incorporated as addendums if agreed to by the Parties.

If a conflict or ambiguity arises after the Addendum to Contract Award have been negotiated and agreed to, the Addendum to Contract Award shall be interpreted as follows:

1. If only one Party has a particular clause then that clause shall control;
2. If both Parties have a similar clause, but the clauses do not conflict, the clauses shall be read together;
3. If both Parties have a similar clause, but the clauses conflict, the State's clause shall control.

A. GENERAL

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

The contract resulting from this solicitation shall incorporate the following documents:

1. Request for Proposal and Addenda;
2. Amendments to the solicitation;
3. Questions and Answers;
4. Bidder's proposal (Solicitation and properly submitted documents);
5. The executed Contract and Addendum One to Contract, if applicable; and,
6. Amendments/Addendums to the Contract.

These documents constitute the entirety of the contract.

Unless otherwise specifically stated in a future contract amendment, in case of any conflict between the incorporated documents, the documents shall govern in the following order of preference with number one (1) receiving preference over all other documents and with each lower numbered document having preference over any higher numbered document: 1) Amendment to the executed Contract with the most recent dated amendment having the highest priority, 2) executed Contract and any attached Addenda, 3) Amendments to solicitation and any Questions and Answers, 4) the original solicitation document and any Addenda, and 5) the bidder's submitted Proposal.

Any ambiguity or conflict in the contract discovered after its execution, not otherwise addressed herein, shall be resolved in accordance with the rules of contract interpretation as established in the State of Nebraska.

B. NOTIFICATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

Contractor and State shall identify the contract manager who shall serve as the point of contact for the executed contract.

Communications regarding the executed contract shall be in writing and shall be deemed to have been given if delivered personally or mailed, by U.S. Mail, postage prepaid, return receipt requested, to the parties at their respective addresses set forth below, or at such other addresses as may be specified in writing by either of the parties. All notices, requests, or communications shall be deemed effective upon personal delivery or five (5) calendar days following deposit in the mail.

Either party may change its address for notification purposes by giving notice of the change, and setting forth the new address and an effective date.

C. BUYER'S REPRESENTATIVE

The State reserves the right to appoint a Buyer's Representative to manage (or assist the Buyer in managing) the contract on behalf of the State. The Buyer's Representative will be appointed in writing, and the appointment document will specify the extent of the Buyer's Representative authority and responsibilities. If a Buyer's Representative is appointed, the Contractor will be provided a copy of the appointment document, and is required to cooperate accordingly with the Buyer's Representative. The Buyer's Representative has no authority to bind the State to a contract, amendment, addendum, or other change or addition to the contract.

D. GOVERNING LAW (Statutory)

Notwithstanding any other provision of this contract, or any amendment or addendum(s) entered into contemporaneously or at a later time, the parties understand and agree that, (1) the State of Nebraska is a sovereign state and its authority to contract is therefore subject to limitation by the State's Constitution, statutes, common law, and regulation; (2) this contract will be interpreted and enforced under the laws of the State of Nebraska; (3) any action to enforce the provisions of this agreement must be brought in the State of Nebraska per state law; (4) the person signing this contract on behalf of the State of Nebraska does not have the authority to waive the State's sovereign immunity, statutes, common law, or regulations; (5) the indemnity, limitation of liability, remedy, and other similar provisions of the final contract, if any, are entered into subject to the State's Constitution, statutes, common law, regulations, and sovereign immunity; and, (6) all terms and conditions of the final contract, including but not limited to the clauses concerning third party use, licenses, warranties, limitations of liability, governing law and venue, usage verification, indemnity, liability, remedy or other similar provisions of the final contract are entered into specifically subject to the State's Constitution, statutes, common law, regulations, and sovereign immunity.

The Parties must comply with all applicable local, state and federal laws, ordinances, rules, orders, and regulations.

E. BEGINNING OF WORK

The bidder shall not commence any billable work until a valid contract has been fully executed by the State and the awarded bidder. The awarded bidder will be notified in writing when work may begin.

F. AMENDMENT

This Contract may be amended in writing, within scope, upon the agreement of both parties.

G. CHANGE ORDERS OR SUBSTITUTIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

The State and the Contractor, upon the written agreement, may make changes to the contract within the general scope of the solicitation. Changes may involve specifications, the quantity of work, or such other items as the State may find necessary or desirable. Corrections of any deliverable, service, or work required pursuant to the contract shall not be deemed a change. The Contractor may not claim forfeiture of the contract by reasons of such changes.

The Contractor shall prepare a written description of the work required due to the change and an itemized cost sheet for the change. Changes in work and the amount of compensation to be paid to the Contractor shall be determined in accordance with applicable unit prices if any, a pro-rated value, or through negotiations. The State shall not incur a price increase for changes that should have been included in the Contractor's proposal, were foreseeable, or result from difficulties with or failure of the Contractor's proposal or performance.

No change shall be implemented by the Contractor until approved by the State, and the Contract is amended to reflect the change and associated costs, if any. If there is a dispute regarding the cost, but both parties agree that immediate implementation is necessary, the change may be implemented, and cost negotiations may continue with both Parties retaining all remedies under the contract and law.

In the event any product is discontinued or replaced upon mutual consent during the contract period or prior to delivery, the State reserves the right to amend the contract or purchase order to include the alternate product at the same price.

*****Contractor will not substitute any item that has been awarded without prior written approval of SPB*****

H. VENDOR PERFORMANCE REPORT(S)

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

The State may document any instance(s) of products or services delivered or performed which exceed or fail to meet the terms of the purchase order, contract, and/or solicitation specifications. The State Purchasing Bureau may contact the Vendor regarding any such report. Vendor performance report(s) will become a part of the permanent record of the Vendor.

I. NOTICE OF POTENTIAL CONTRACTOR BREACH

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

If Contractor breaches the contract or anticipates breaching the contract, the Contractor shall immediately give written notice to the State. The notice shall explain the breach or potential breach, a proposed cure, and may include a request for a waiver of the breach if so desired. The State may, in its discretion, temporarily or permanently waive the breach. By granting a waiver, the State does not forfeit any rights or remedies to which the State is entitled by law or equity, or pursuant to the provisions of the contract. Failure to give immediate notice, however, may be grounds for denial of any request for a waiver of a breach.

J. BREACH

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

Either Party may terminate the contract, in whole or in part, if the other Party breaches its duty to perform its obligations under the contract in a timely and proper manner. Termination requires written notice of default and a thirty (30) calendar day (or longer at the non-breaching Party's discretion considering the gravity and nature of the default) cure period. Said notice shall be delivered by Certified Mail, Return Receipt Requested, or in person with proof of delivery. Allowing time to cure a failure or breach of contract does not waive the right to immediately terminate the contract for the same or different contract breach which may occur at a different time. In case of default of the Contractor, the State may contract the service from other sources and hold the Contractor responsible for any excess cost occasioned thereby. OR In case of breach by the Contractor, the State may, without unreasonable delay, make a good faith effort to make a reasonable purchase or contract to purchase goods in substitution of those due from the contractor. The State may recover from the Contractor as damages the difference between the costs of covering the breach. Notwithstanding any clause to the contrary, the State may also recover the contract price together with any incidental or consequential damages defined in UCC Section 2-715, but less expenses saved in consequence of Contractor's breach.

The State's failure to make payment shall not be a breach, and the Contractor shall retain all available statutory remedies and protections.

K. NON-WAIVER OF BREACH

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

The acceptance of late performance with or without objection or reservation by a Party shall not waive any rights of the Party nor constitute a waiver of the requirement of timely performance of any obligations remaining to be performed.

L. SEVERABILITY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

If any term or condition of the contract is declared by a court of competent jurisdiction to be illegal or in conflict with any law, the validity of the remaining terms and conditions shall not be affected, and the rights and obligations of the parties shall be construed and enforced as if the contract did not contain the provision held to be invalid or illegal.

M. INDEMNIFICATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

1. GENERAL

The Contractor agrees to defend, indemnify, and hold harmless the State and its employees, volunteers, agents, and its elected and appointed officials ("the indemnified parties") from and against any and all third party claims, liens, demands, damages, liability, actions, causes of action, losses, judgments, costs, and expenses of every nature, including investigation costs and expenses, settlement costs, and attorney fees and expenses ("the claims"), sustained or asserted against the State for personal injury, death, or property loss or damage, arising out of, resulting from, or attributable to the willful misconduct, negligence, error, or omission of the Contractor, its employees, subcontractors, consultants, representatives, and agents, resulting from this contract, except to the extent such Contractor liability is attenuated by any action of the State which directly and proximately contributed to the claims.

2. INTELLECTUAL PROPERTY (Optional)

The Contractor agrees it will, at its sole cost and expense, defend, indemnify, and hold harmless the indemnified parties from and against any and all claims, to the extent such claims arise out of, result from, or are attributable to, the actual or alleged infringement or misappropriation of any patent, copyright, trade secret, trademark, or confidential information of any third party by the Contractor or its employees, subcontractors, consultants, representatives, and agents; provided, however, the State gives the Contractor prompt notice in writing of the claim. The Contractor may not settle any infringement claim that will affect the State's use of the Licensed Software without the State's prior written consent, which consent may be withheld for any reason.

If a judgment or settlement is obtained or reasonably anticipated against the State's use of any intellectual property for which the Contractor has indemnified the State, the Contractor shall, at the Contractor's sole cost and expense, promptly modify the item or items which were determined to be infringing, acquire a license or licenses on the State's behalf to provide the necessary rights to the State to eliminate the infringement, or provide the State with a non-infringing substitute that provides the State the same functionality. At the State's election, the actual or anticipated judgment may be treated as a breach of warranty by the Contractor, and the State may receive the remedies provided under this solicitation.

3. PERSONNEL

The Contractor shall, at its expense, indemnify and hold harmless the indemnified parties from and against any claim with respect to withholding taxes, worker's compensation, employee benefits, or any other claim, demand, liability, damage, or loss of any nature relating to any of the personnel, including subcontractor's and their employees, provided by the Contractor.

4. SELF-INSURANCE

The State of Nebraska is self-insured for any loss and purchases excess insurance coverage pursuant to Neb. Rev. Stat. § 81-8,239.01 (Reissue 2008). If there is a presumed loss under the provisions of this agreement, Contractor may file a claim with the Office of Risk Management pursuant to Neb. Rev. Stat. §§ 81-8,829 – 81-8,306 for review by the State Claims Board. The State retains all rights and immunities under the State Miscellaneous (§ 81-8,294), Tort (§ 81-8,209), and Contract Claim Acts (§ 81-8,302), as outlined in Neb. Rev. Stat. § 81-8,209 et seq. and under any other provisions of law and accepts liability under this agreement to the extent provided by law.

5. The Parties acknowledge that Attorney General for the State of Nebraska is required by statute to represent the legal interests of the State, and that any provision of this indemnity clause is subject to the statutory authority of the Attorney General.

N. ATTORNEY'S FEES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

In the event of any litigation, appeal, or other legal action to enforce any provision of the contract, the Parties agree to pay all expenses of such action, as permitted by law and if ordered by the court, including attorney's fees and costs, if the other Party prevails.

O. PERFORMANCE BOND

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

The Contractor maybe required to supply a bond executed by a corporation authorized to contract surety in the State of Nebraska, payable to the State of Nebraska, which shall be valid for the life of the contract to include any renewal and/or extension periods. The amount of the bond must be $500,000. The bond will guarantee that the Contractor will faithfully perform all requirements, terms and conditions of the contract. Failure to comply shall be grounds for forfeiture of bond as liquidated damages. Amount of forfeiture will be determined by the agency based on loss to the State. The bond will be returned when the contract has been satisfactorily completed as solely determined by the State, after termination or expiration of the contract.

P. ASSIGNMENT, SALE, OR MERGER

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

Either Party may assign the contract upon mutual written agreement of the other Party. Such agreement shall not be unreasonably withheld.

The Contractor retains the right to enter into a sale, merger, acquisition, internal reorganization, or similar transaction involving Contractor’s business. Contractor agrees to cooperate with the State in executing amendments to the contract to allow for the transaction. If a third party or entity is involved in the transaction, the Contractor will remain responsible for performance of the contract until such time as the person or entity involved in the transaction agrees in writing to be contractually bound by this contract and perform all obligations of the contract.

Q. CONTRACTING WITH OTHER NEBRASKA POLITICAL SUB-DIVISIONS OF THE STATE OR ANOTHER STATE

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

The Contractor may, but shall not be required to, allow agencies, as defined in Neb. Rev. Stat. §81-145, to use this contract. The terms and conditions, including price, of the contract may not be amended. The State shall not be contractually obligated or liable for any contract entered into pursuant to this clause. A listing of Nebraska political subdivisions may be found at the website of the Nebraska Auditor of Public Accounts.

The Contractor may, but shall not be required to, allow other states, agencies or divisions of other states, or political subdivisions of other states to use this contract. The terms and conditions, including price, of this contract shall apply to any such contract, but may be amended upon mutual consent of the Parties. The State of Nebraska shall not be contractually or otherwise obligated or liable under any contract entered into pursuant to this clause. The State shall be notified if a contract is executed based upon this contract.

R. FORCE MAJEURE

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

Neither Party shall be liable for any costs or damages, or for default resulting from its inability to perform any of its obligations under the contract due to a natural or manmade event outside the control and not the fault of the affected Party ("Force Majeure Event"). The Party so affected shall immediately make a written request for relief to the other Party, and shall have the burden of proof to justify the request. The other Party may grant the relief requested; relief may not be unreasonably withheld. Labor disputes with the impacted Party's own employees will not be considered a Force Majeure Event.

S. CONFIDENTIALITY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

All materials and information provided by the Parties or acquired by a Party on behalf of the other Party shall be regarded as confidential information. All materials and information provided or acquired shall be handled in accordance with federal and state law, and ethical standards. Should said confidentiality be breached by a Party, the Party shall notify the other Party immediately of said breach and take immediate corrective action.

It is incumbent upon the Parties to inform their officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a (i)(1), which is made applicable by 5 U.S.C. 552a (m)(1), provides that any officer or employee, who by virtue of his/her employment or official position has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

T. EARLY TERMINATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

The contract may be terminated as follows:

1. The State and the Contractor, by mutual written agreement, may terminate the contract at any time.

2. The State, in its sole discretion, may terminate the contract for any reason upon thirty (30) calendar day's written notice to the Contractor. Such termination shall not relieve the Contractor of warranty or other service obligations incurred under the terms of the contract. In the event of termination the Contractor shall be entitled to payment, determined on a pro rata basis, for products or services satisfactorily performed or provided.

3. The State may terminate the contract immediately for the following reasons:

- **a.** if directed to do so by statute;
- **b.** Contractor has made an assignment for the benefit of creditors, has admitted in writing its inability to pay debts as they mature, or has ceased operating in the normal course of business;
- **c.** a trustee or receiver of the Contractor or of any substantial part of the Contractor's assets has been appointed by a court;
- **d.** fraud, misappropriation, embezzlement, malfeasance, misfeasance, or illegal conduct pertaining to performance under the contract by its Contractor, its employees, officers, directors, or shareholders;
- **e.** an involuntary proceeding has been commenced by any Party against the Contractor under any one of the chapters of Title 11 of the United States Code and (i) the proceeding has been pending for at least sixty (60) calendar days; or (ii) the Contractor has consented, either expressly or by operation of law, to the entry of an order for relief; or (iii) the Contractor has been decreed or adjudged a debtor;
- **f.** a voluntary petition has been filed by the Contractor under any of the chapters of Title 11 of the United States Code;
- **g.** Contractor intentionally discloses confidential information;
- **h.** Contractor has or announces it will discontinue support of the deliverable; and,
- **i.** In the event funding is no longer available.

U. CONTRACT CLOSEOUT

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

Upon contract closeout for any reason the Contractor shall within 30 calendar days, unless stated otherwise herein:

1. Transfer all completed or partially completed deliverables to the State;
2. Transfer ownership and title to all completed or partially completed deliverables to the State;
3. Return to the State all information and data, unless the Contractor is permitted to keep the information or data by contract or rule of law. Contractor may retain one copy of any information or data as required to comply with applicable work product documentation standards or as are automatically retained in the course of Contractor's routine back up procedures;
4. Cooperate with any successor Contactor, person or entity in the assumption of any or all of the obligations of this contract;
5. Cooperate with any successor Contactor, person or entity with the transfer of information or data related to this contract;
6. Return or vacate any state owned real or personal property; and,

7. Return all data in a mutually acceptable format and manner.

Nothing in this Section should be construed to require the Contractor to surrender intellectual property, real or personal property, or information or data owned by the Contractor for which the State has no legal claim.

III. CONTRACTOR DUTIES

V. INDEPENDENT CONTRACTOR / OBLIGATIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

It is agreed that the Contractor is an independent contractor and that nothing contained herein is intended or should be construed as creating or establishing a relationship of employment, agency, or a partnership.

The Contractor is solely responsible for fulfilling the contract. The Contractor or the Contractor's representative shall be the sole point of contact regarding all contractual matters.

The Contractor shall secure, at its own expense, all personnel required to perform the services under the contract. The personnel the Contractor uses to fulfill the contract shall have no contractual or other legal relationship with the State; they shall not be considered employees of the State and shall not be entitled to any compensation, rights or benefits from the State, including but not limited to, tenure rights, medical and hospital care, sick and vacation leave, severance pay, or retirement benefits.

By-name personnel commitments made in the Contractor's proposal shall not be changed without the prior written approval of the State. Replacement of these personnel, if approved by the State, shall be with personnel of equal or greater ability and qualifications.

All personnel assigned by the Contractor to the contract shall be employees of the Contractor or a subcontractor, and shall be fully qualified to perform the work required herein. Personnel employed by the Contractor or a subcontractor to fulfill the terms of the contract shall remain under the sole direction and control of the Contractor or the subcontractor respectively.

With respect to its employees, the Contractor agrees to be solely responsible for the following:

i. Any and all pay, benefits, and employment taxes and/or other payroll withholding;
ii. Any and all vehicles used by the Contractor's employees, including all insurance required by state law;
iii. Damages incurred by Contractor's employees within the scope of their duties under the contract;
iv. Maintaining Workers' Compensation and health insurance that complies with state and federal law and submitting any reports on such insurance to the extent required by governing law;
v. Determining the hours to be worked and the duties to be performed by the Contractor's employees; and,
vi. All claims on behalf of any person arising out of employment or alleged employment (including without limit claims of discrimination alleged against the Contractor, its officers, agents, or subcontractors or subcontractor's employees).

If the Contractor intends to utilize any subcontractor, the subcontractor's level of effort, tasks, and time allocation should be clearly defined in the bidder's proposal. The Contractor shall agree that it will not utilize any subcontractors not specifically included in its proposal in the performance of the contract without the prior written authorization of the State.

The State reserves the right to require the Contractor to reassign or remove from the project any Contractor or subcontractor employee.

Contractor shall insure that the terms and conditions contained in any contract with a subcontractor does not conflict with the terms and conditions of this contract.

The Contractor shall include a similar provision, for the protection of the State, in the contract with any subcontractor engaged to perform work on this contract.

W. EMPLOYEE WORK ELIGIBILITY STATUS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within	NOTES/COMMENTS:

		Solicitation Response (Initial)	
MB			

The Contractor is required and hereby agrees to use a federal immigration verification system to determine the work eligibility status of employees physically performing services within the State of Nebraska. A federal immigration verification system means the electronic verification of the work authorization program authorized by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, 8 U.S.C. 1324a, known as the E-Verify Program, or an equivalent federal program designated by the United States Department of Homeland Security or other federal agency authorized to verify the work eligibility status of an employee.

If the Contractor is an individual or sole proprietorship, the following applies:

vii. The Contractor must complete the United States Citizenship Attestation Form, available on the Department of Administrative Services website at http://das.nebraska.gov/materiel/purchasing.html.

viii. The completed United States Attestation Form should be submitted with the solicitation response.

ix. If the Contractor indicates on such attestation form that he or she is a qualified alien, the Contractor agrees to provide the US Citizenship and Immigration Services documentation required to verify the Contractor's lawful presence in the United States using the Systematic Alien Verification for Entitlements (SAVE) Program.

x. The Contractor understands and agrees that lawful presence in the United States is required and the Contractor may be disqualified or the contract terminated if such lawful presence cannot be verified as required by Neb. Rev. Stat. §4-108.

X. COMPLIANCE WITH CIVIL RIGHTS LAWS AND EQUAL OPPORTUNITY EMPLOYMENT / NONDISCRIMINATION (Statutory)

The Contractor shall comply with all applicable local, state, and federal statutes and regulations regarding civil rights laws and equal opportunity employment. The Nebraska Fair Employment Practice Act prohibits Contractors of the State of Nebraska, and their subcontractors, from discriminating against any employee or applicant for employment, with respect to hire, tenure, terms, conditions, compensation, or privileges of employment because of race, color, religion, sex, disability, marital status, or national origin (Neb. Rev. Stat. §48-1101 to 48-1125). The Contractor guarantees compliance with the Nebraska Fair Employment Practice Act, and breach of this provision shall be regarded as a material breach of contract. The Contractor shall insert a similar provision in all subcontracts for goods and services to be covered by any contract resulting from this solicitation.

Y. COOPERATION WITH OTHER CONTRACTORS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

Contractor may be required to work with or in close proximity to other contractors or individuals that may be working on same or different projects. The Contractor shall agree to cooperate with such other contractors or individuals, and shall not commit or permit any act which may interfere with the performance of work by any other contractor or individual. Contractor is not required to compromise Contractor's intellectual property or proprietary information unless expressly required to do so by this contract.

Z. PERMITS, REGULATIONS, LAWS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:

MB			

The contract price shall include the cost of all royalties, licenses, permits, and approvals, whether arising from patents, trademarks, copyrights or otherwise, that are in any way involved in the contract. The Contractor shall obtain and pay for all royalties, licenses, and permits, and approvals necessary for the execution of the contract. The Contractor must guarantee that it has the full legal right to the materials, supplies, equipment, software, and other items used to execute this contract.

AA. OWNERSHIP OF INFORMATION AND DATA / DELIVERABLES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

The State shall have the unlimited right to publish, duplicate, use, and disclose all information and data developed or obtained by the Contractor on behalf of the State pursuant to this contract.

The State shall own and hold exclusive title to any deliverable developed as a result of this contract. Contractor shall have no ownership interest or title, and shall not patent, license, or copyright, duplicate, transfer, sell, or exchange, the design, specifications, concept, or deliverable.

BB. INSURANCE REQUIREMENTS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

The Contractor shall throughout the term of the contract maintain insurance as specified herein and provide the State a current Certificate of Insurance/Acord Form (COI) verifying the coverage. The Contractor shall not commence work on the contract until the insurance is in place. If Contractor subcontracts any portion of the Contract the Contractor must, throughout the term of the contract, either:

xi. Provide equivalent insurance for each subcontractor and provide a COI verifying the coverage for the subcontractor;
xii. Require each subcontractor to have equivalent insurance and provide written notice to the State that the Contractor has verified that each subcontractor has the required coverage; or,
xiii. Provide the State with copies of each subcontractor's Certificate of Insurance evidencing the required coverage.

The Contractor shall not allow any subcontractor to commence work until the subcontractor has equivalent insurance. The failure of the State to require a COI, or the failure of the Contractor to provide a COI or require subcontractor insurance shall not limit, relieve, or decrease the liability of the Contractor hereunder.

In the event that any policy written on a claims-made basis terminates or is canceled during the term of the contract or within one (1) year of termination or expiration of the contract, the contractor shall obtain an extended discovery or reporting period, or a new insurance policy, providing coverage required by this contract for the term of the contract and one (1) year following termination or expiration of the contract.

If by the terms of any insurance a mandatory deductible is required, or if the Contractor elects to increase the mandatory deductible amount, the Contractor shall be responsible for payment of the amount of the deductible in the event of a paid claim.

Notwithstanding any other clause in this Contract, the State may recover up to the liability limits of the insurance policies required herein.

1. WORKERS' COMPENSATION INSURANCE

The Contractor shall take out and maintain during the life of this contract the statutory Workers' Compensation and Employer's Liability Insurance for all of the contactors' employees to be engaged in work on the project under this contract and, in case any such work is sublet, the Contractor shall require the subcontractor similarly to provide Worker's Compensation and Employer's Liability Insurance for all of the subcontractor's employees to be engaged in such work. This policy shall be written to meet the statutory requirements for the state in which the work is to be performed, including Occupational Disease. **The policy shall include a waiver of subrogation in favor of the State. The COI shall contain the mandatory COI subrogation waiver language found hereinafter**. The amounts of such insurance shall not be less than the limits stated hereinafter. For employees working in the State of Nebraska, the policy must be written by an entity authorized by the State of Nebraska Department of Insurance to write Workers' Compensation and Employer's Liability Insurance for Nebraska employees.

xiv. COMMERCIAL GENERAL LIABILITY INSURANCE AND COMMERCIAL AUTOMOBILE LIABILITY INSURANCE

The Contractor shall take out and maintain during the life of this contract such Commercial General Liability Insurance and Commercial Automobile Liability Insurance as shall protect Contractor and any subcontractor performing work covered by this contract from claims for damages for bodily injury, including death, as well as from claims for property damage, which may arise from operations under this contract, whether such operation be by the Contractor or by any subcontractor or by anyone directly or indirectly employed by either of them, and the amounts of such insurance shall not be less than limits stated hereinafter.

The Commercial General Liability Insurance shall be written on an **occurrence basis**, and provide Premises/Operations, Products/Completed Operations, Independent Contractors, Personal Injury, and Contractual Liability coverage. **The policy shall include the State, and others as required by the contract documents, Additional Insured(s). This policy shall be primary, and any insurance or self-insurance carried by the State shall be considered secondary and non-contributory**. **The COI shall contain the mandatory COI liability waiver language found hereinafter.** The Commercial Automobile Liability Insurance shall be written to cover all Owned, Non-owned, and Hired vehicles.

REQUIRED INSURANCE COVERAGE	
COMMERCIAL GENERAL LIABILITY	
General Aggregate	$2,000,000
Products/Completed Operations Aggregate	$2,000,000
Personal/Advertising Injury	$1,000,000 per occurrence
Bodily Injury/Property Damage	$1,000,000 per occurrence
Medical Payments	$10,000 any one person
Damage to Rented Premises (Fire)	$300,000 each occurrence
Contractual	Included
XCU Liability (Explosion, Collapse, and Underground Damage)	Included
Independent Contractors	Included
Abuse & Molestation	Included
If higher limits are required, the Umbrella/Excess Liability limits are allowed to satisfy the higher limit.	
WORKER'S COMPENSATION	
Employers Liability Limits	$500K/$500K/$500K
Statutory Limits- All States	Statutory - State of Nebraska
Voluntary Compensation	Statutory
COMMERCIAL AUTOMOBILE LIABILITY	
Bodily Injury/Property Damage	$1,000,000 combined single limit
Include All Owned, Hired & Non-Owned Automobile liability	Included
Motor Carrier Act Endorsement	Where Applicable
UMBRELLA/EXCESS LIABILITY	
Over Primary Insurance	$2,000,000 per occurrence
PROFESSIONAL LIABILITY	
All Other Professional Liability (Errors & Omissions)	$1,000,000 Per Claim / Aggregate
COMMERCIAL CRIME	
Crime/Employee Dishonesty Including 3rd Party Fidelity	$1,000,000
CYBER LIABILITY	
Breach of Privacy, Security Breach, Denial of Service, Remediation, Fines and Penalties	$10,000,000
MANDATORY COI SUBROGATION WAIVER LANGUAGE	
"Workers' Compensation policy shall include a waiver of subrogation in favor of the State of Nebraska."	
MANDATORY COI LIABILITY WAIVER LANGUAGE	
"Commercial General Liability & Commercial Automobile Liability policies shall name the State of Nebraska as an Additional Insured and the policies shall be primary and any insurance or self-insurance carried by the State shall be considered secondary and non-contributory as additionally insured."	

xv. EVIDENCE OF COVERAGE

The Contractor shall furnish the Contract Manager, with a certificate of insurance coverage complying with the above requirements prior to beginning work at:

Public Service Commission
Attn: State 911 Director
PO Box 94927
Lincoln, NE 68509

These certificates or the cover sheet shall reference the RFP number, and the certificates shall include the name of the company, policy numbers, effective dates, dates of expiration, and amounts and types of coverage afforded. If the State is damaged by the failure of the Contractor to maintain such insurance, then the Contractor shall be responsible for all reasonable costs properly attributable thereto.

Reasonable notice of cancellation of any required insurance policy must be submitted to the contract manager as listed above when issued and a new coverage binder shall be submitted immediately to ensure no break in coverage.

xvi. DEVIATIONS

The insurance requirements are subject to limited negotiation. Negotiation typically includes, but is not necessarily limited to, the correct type of coverage, necessity for Workers' Compensation, and the type of automobile coverage carried by the Contractor.

CC. ANTITRUST

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

The Contractor hereby assigns to the State any and all claims for overcharges as to goods and/or services provided in connection with this contract resulting from antitrust violations which arise under antitrust laws of the United States and the antitrust laws of the State.

DD. CONFLICT OF INTEREST

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

By submitting a proposal, bidder certifies that no relationship exists between the bidder and any person or entity which either is, or gives the appearance of, a conflict of interest related to this Request for Proposal or project.

Bidder further certifies that bidder will not employ any individual known by bidder to have a conflict of interest nor shall bidder take any action or acquire any interest, either directly or indirectly, which will conflict in any manner or degree with the performance of its contractual obligations hereunder or which creates an actual or appearance of conflict of interest.

If there is an actual or perceived conflict of interest, bidder shall provide with its proposal a full disclosure of the facts describing such actual or perceived conflict of interest and a proposed mitigation plan for consideration. The State will then consider such disclosure and proposed mitigation plan and either approve or reject as part of the overall bid evaluation.

EE. STATE PROPERTY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

The Contractor shall be responsible for the proper care and custody of any State-owned property which is furnished for the Contractor's use during the performance of the contract. The Contractor shall reimburse the State for any loss or damage of such property; normal wear and tear is expected.

FF. SITE RULES AND REGULATIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:

MB			

The Contractor shall use its best efforts to ensure that its employees, agents, and subcontractors comply with site rules and regulations while on State or any government premises. If the Contractor must perform on-site work outside of the daily operational hours set forth by the State, it must make arrangements with the State or any government to ensure access to the facility and the equipment has been arranged. No additional payment will be made by the State on the basis of lack of access, unless the State fails to provide access as agreed to in writing between the State and the Contractor.

GG. ADVERTISING

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

The Contractor agrees not to refer to the contract award in advertising in such a manner as to state or imply that the company or its goods or services are endorsed or preferred by the State. Any publicity releases pertaining to the project shall not be issued without prior written approval from the State.

HH. NEBRASKA TECHNOLOGY ACCESS STANDARDS (Statutory)

Contractor shall review the Nebraska Technology Access Standards, found at http://nitc.nebraska.gov/standards/2-201.html and ensure that products and/or services provided under the contract are in compliance or will comply with the applicable standards to the greatest degree possible. In the event such standards change during the Contractor's performance, the State may create an amendment to the contract to request the contract comply with the changed standard at a cost mutually acceptable to the parties.

II. DISASTER RECOVERY/BACK UP PLAN

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

The Contractor shall have a disaster recovery and back-up plan, of which a copy should be provided upon request to the State, which includes, but is not limited to equipment, personnel, facilities, and transportation, in order to continue delivery of goods and services as specified under the specifications in the contract in the event of a disaster.

JJ. DRUG POLICY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

Contractor certifies it maintains a drug free work place environment to ensure worker safety and workplace integrity. Contractor agrees to provide a copy of its drug free workplace policy at any time upon request by the State.

KK. WARRANTY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

Despite any clause to the contrary, the Contractor represents and warrants that its services hereunder shall be performed by competent personnel and shall be of professional quality consistent with generally accepted industry standards for the performance of such services and shall comply in all respects with the requirements of this Agreement. For any breach of this warranty, the Contractor shall, for a period of ninety (90) calendar days from performance of the service, perform the services again, at no cost to the State, or if Contractor is unable to perform the services as warranted, Contractor shall reimburse the State all fees paid to Contractor for the unsatisfactory services. The rights and remedies of the parties under this warranty are in addition to any other rights and remedies of the parties provided by law or equity, including, without limitation actual damages, and, as applicable and awarded under the law, to a prevailing party, reasonable attorneys' fees and costs.

IV. PAYMENT

LL. PROHIBITION AGAINST ADVANCE PAYMENT (Statutory)

Neb. Rev. Stat. §§81-2403 states, "[n]o goods or services shall be deemed to be received by an agency until all such goods or services are completely delivered and finally accepted by the agency."

MM. TAXES (Statutory)

The State is not required to pay taxes and assumes no such liability as a result of this solicitation. The Contractor may request a copy of the Nebraska Department of Revenue, Nebraska Resale or Exempt Sale Certificate for Sales Tax Exemption, Form 13 for their records. Any property tax payable on the Contractor's equipment which may be installed in a state-owned facility is the responsibility of the Contractor

NN. INVOICES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

Invoices for payments must be submitted by the Contractor to the agency requesting the services with sufficient detail to support payment. Public Service Commission State 911 Director 1200 N St. Lincoln, NE 68509. The terms and conditions included in the Contractor's invoice shall be deemed to be solely for the convenience of the parties. No terms or conditions of any such invoice shall be binding upon the State, and no action by the State, including without limitation the payment of any such invoice in whole or in part, shall be construed as binding or estopping the State with respect to any such term or condition, unless the invoice term or condition has been previously agreed to by the State as an amendment to the contract.

OO. INSPECTION AND APPROVAL

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

Final inspection and approval of all work required under the contract shall be performed by the designated State officials.

The State and/or its authorized representatives shall have the right to enter any premises where the Contractor or subcontractor duties under the contract are being performed, and to inspect, monitor or otherwise evaluate the work being performed. All inspections and evaluations shall be at reasonable times and in a manner that will not unreasonably delay work.

PP. PAYMENT (Statutory)

Payment will be made by the responsible agency in compliance with the State of Nebraska Prompt Payment Act (See Neb. Rev. Stat. §81-2403). The State may require the Contractor to accept payment by electronic means such as ACH deposit. In no event shall the State be responsible or liable to pay for any goods and services provided by the Contractor prior to the Effective Date of the contract, and the Contractor hereby waives any claim or cause of action for any such services.

QQ. LATE PAYMENT (Statutory)

The Contractor may charge the responsible agency interest for late payment in compliance with the State of Nebraska Prompt Payment Act (See Neb. Rev. Stat. §81-2401 through 81-2408).

RR. SUBJECT TO FUNDING / FUNDING OUT CLAUSE FOR LOSS OF APPROPRIATIONS (Statutory)

The State's obligation to pay amounts due on the Contract for a fiscal years following the current fiscal year is contingent upon legislative appropriation of funds. Should said funds not be appropriated, the State may terminate the contract with respect to those payments for the fiscal year(s) for which such funds are not appropriated. The

State will give the Contractor written notice thirty (30) calendar days prior to the effective date of termination. All obligations of the State to make payments after the termination date will cease. The Contractor shall be entitled to receive just and equitable compensation for any authorized work which has been satisfactorily completed as of the termination date. In no event shall the Contractor be paid for a loss of anticipated profit.

SS. RIGHT TO AUDIT (First Paragraph is Statutory)

The State shall have the right to audit the Contractor's performance of this contract upon a thirty (30) calendar days' written notice. Contractor shall utilize generally accepted accounting principles, and shall maintain the accounting records, and other records and information relevant to the contract (Information) to enable the State to audit the contract. (Neb. Rev. Stat. §84-304 et seq.) The State may audit and the Contractor shall maintain, the Information during the term of the contract and for a period of five (5) years after the completion of this contract or until all issues or litigation are resolved, whichever is later. The Contractor shall make the Information available to the State at Contractor's place of business or a location acceptable to both Parties during normal business hours. If this is not practical or the Contractor so elects, the Contractor may provide electronic or paper copies of the Information. The State reserves the right to examine, make copies of, and take notes on any Information relevant to this contract, regardless of the form or the Information, how it is stored, or who possesses the Information. Under no circumstance will the Contractor be required to create or maintain documents not kept in the ordinary course of contractor's business operations, nor will contractor be required to disclose any information, including but not limited to product cost data, which is confidential or proprietary to contractor.

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
MB			

The Parties shall pay their own costs of the audit unless the audit finds a previously undisclosed overpayment by the State. If a previously undisclosed overpayment exceeds one-half of one percent (.5%) of the total contract billings, or if fraud, material misrepresentations, or non-performance is discovered on the part of the Contractor, the Contractor shall reimburse the State for the total costs of the audit. Overpayments and audit costs owed to the State shall be paid within ninety (90) days of written notice of the claim. The Contractor agrees to correct any material weaknesses or condition found as a result of the audit.

RFP 6264 Z1

Section III: Project Description and Scope of Work

Option B

NGA 911

June, 2020

Table of Contents

A. BACKGROUND AND PROJECT SCOPE 2
B. COMPOSITON OF THE REQUEST FOR PROPOSAL 2
1. Option A: Deployment of ESInet 2
a. Public Safety-Grade ..... **Error! Bookmark not defined.**
b. Cost Effective and Consistent Level of Service ..... **Error! Bookmark not defined.**
c. Phased Implementation Approach ..... **Error! Bookmark not defined.**
d. Cooperation and Coordination ..... **Error! Bookmark not defined.**
C. BIDDER REQUIREMENTS 4
1. Requirements with Response 5
a. Configuration Solution 5
b. Attachments 8
c. Appendices 8
d. Brochures 8
D. GENERAL REQUIREMENTS - TECHNICAL 9
1. Commission Requirements 9
a. Industry Standards 9
b. Public Safety-Grade Definition 10

A. BACKGROUND AND PROJECT SCOPE

NGA 911 understands that the Nebraska Public Service Commission, State 911 Department (The Commission) is seeking to build an Emergency Service Internet Protocol (IP) Network (ESInet) and Next Generation Core Services (NGCS) to advance Next Generation 911 (NG9-1-1) throughout the state of Nebraska.

The PSAPs in Nebraska have joined to form regions in which they share call-handling equipment (CHE). The CHE server-side software is hosted at a central location in each region; all of the call-taker station clients at each PSAP in the region then access the server remotely. The Commission is looking to build a statewide public safety grade ESInet that connects all the regional PSAPs host locations to an NGCS. NGA 911 understands that its plans will need to be flexible in dimensioning these systems as independent PSAPs join existing regions and/or combine to create a new region in the next 12 to 18 months.

B. COMPOSITON OF THE REQUEST FOR PROPOSAL

1. Option B: Deployment of Next Generation Core Service (NGCS)

NGA 911 proposes to design, deploy, and operate an NGCS for the state of Nebraska in support of The Commission's goal of connecting all of the regional hosts into a single coherent Next Generation 911 system.

a. Managed Core Services

NGA 911 is proposing an NGCS that exceeds public safety-grade standards as defined by Nebraska in III.D.2 of this RFP. Not only will it be built compliant with all the relevant standards listed in III.D.1 of this RFP but it will significantly exceed The Commission's requirements of 5 9s for reliability and availability. NGA 911 can exceed these requirements by hosting the NGCS almost entirely in the cloud on our partner Amazon Web Services' (AWS) platform.

With 8 separate instances of the NGCS (each of which can handle the entire traffic flow from the Nebraska) running simultaneously in data centers, geographically widely dispersed, NGA 911 provides unprecedented redundancy and resiliency to NG9-1-1 emergency communications.

As most of the solution is deployed as software instances on virtual servers it is very easy to update the software as well as scale the hardware platform to meet new traffic and computing demands as NG9-1-1 services evolve. Our extreme cloud-shared redundancy ensures that Nebraska's NG9-1-1 system will not go down during the change event in the NGCS.

NGA 911 is offering its solution to The Commission as a complete managed service for Nebraska under SLA. The solution is monitored 24X7X365 by our NOC/SOC, which is run by our partners Fujitsu.

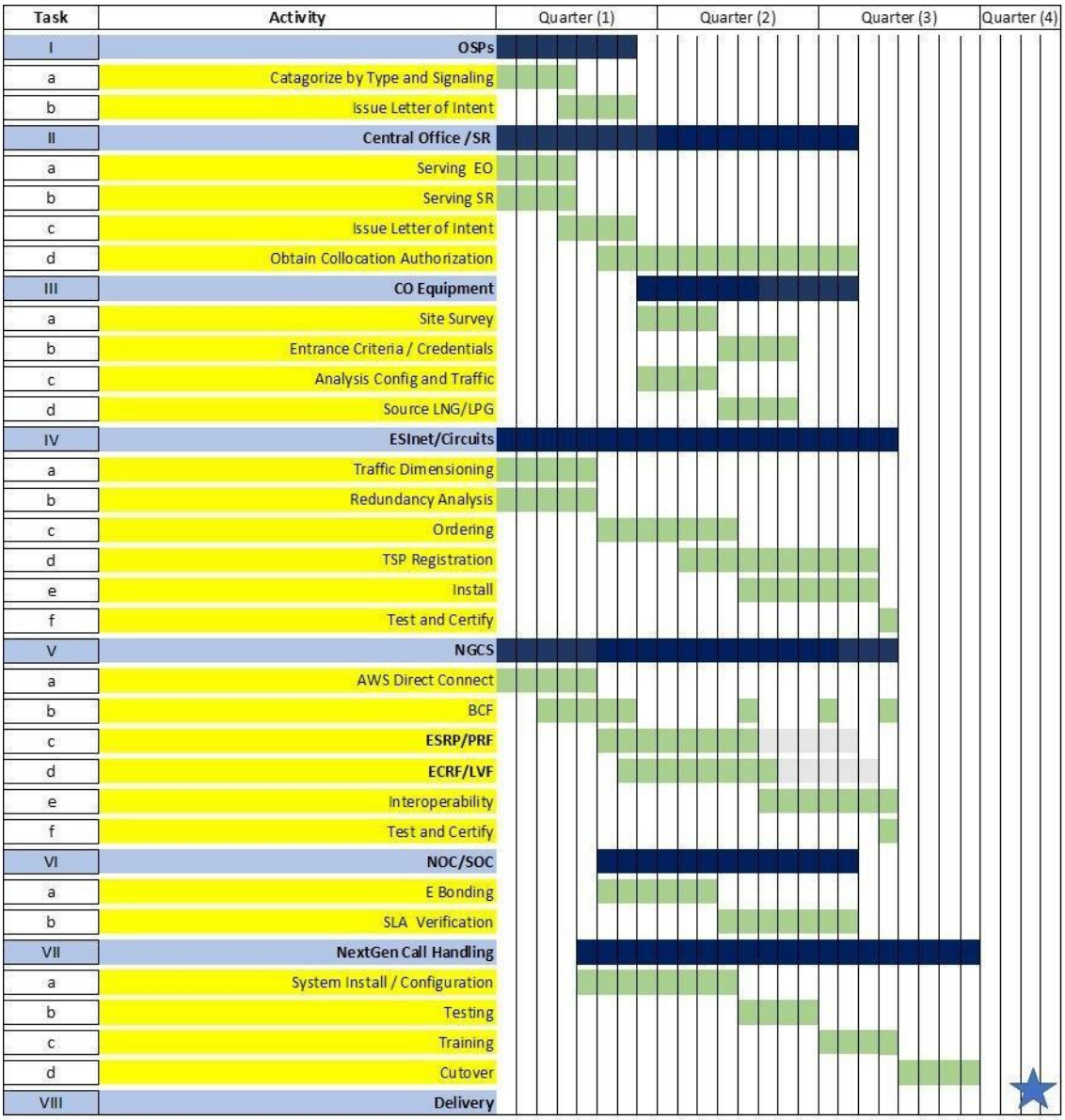
b. Transition to GIS

NGA 911 provides a smooth transition for Nebraska to ultimately do geospatial 911 call routing. OSPs are in various states of transition regarding their ability to pass geographic coordinate locations of the callers. To accommodate these different levels of NG sophistication, we have implemented a Location Database (LDB) which combines a fully functional legacy ALI DBMS with a fully functional NENA i3 compliant LIS. This combined NGCS element will allow call routing to be done either by civic address through ALI/MSAG or by geospatial means through the LIS depending on the capabilities of the OSP and the information passed to the NGCS.

c. Transition Timeline

NGA 911 plans to complete the State's cutover to the ESInet and NGCS in 9 months. The actual timeline may deviate somewhat depending on the cooperation of the ESInet provider and the OSPs but based on previous experience, although aggressive, this timeline is achievable. We intend to deploy, test and validate most of the NGCS before cutover. As we cutover PSAPs we should only have a 6 to 8 week overlap between the SR network and the NGCS.

Below is a high-level timeline of our approach to the deployment of the NGCS; because of the necessarily tight dependencies between the ESInet and the NGCS we have included in this Gantt chart reasonable duration estimates for the ESInet deployment functions.



d. Multimedia Capability

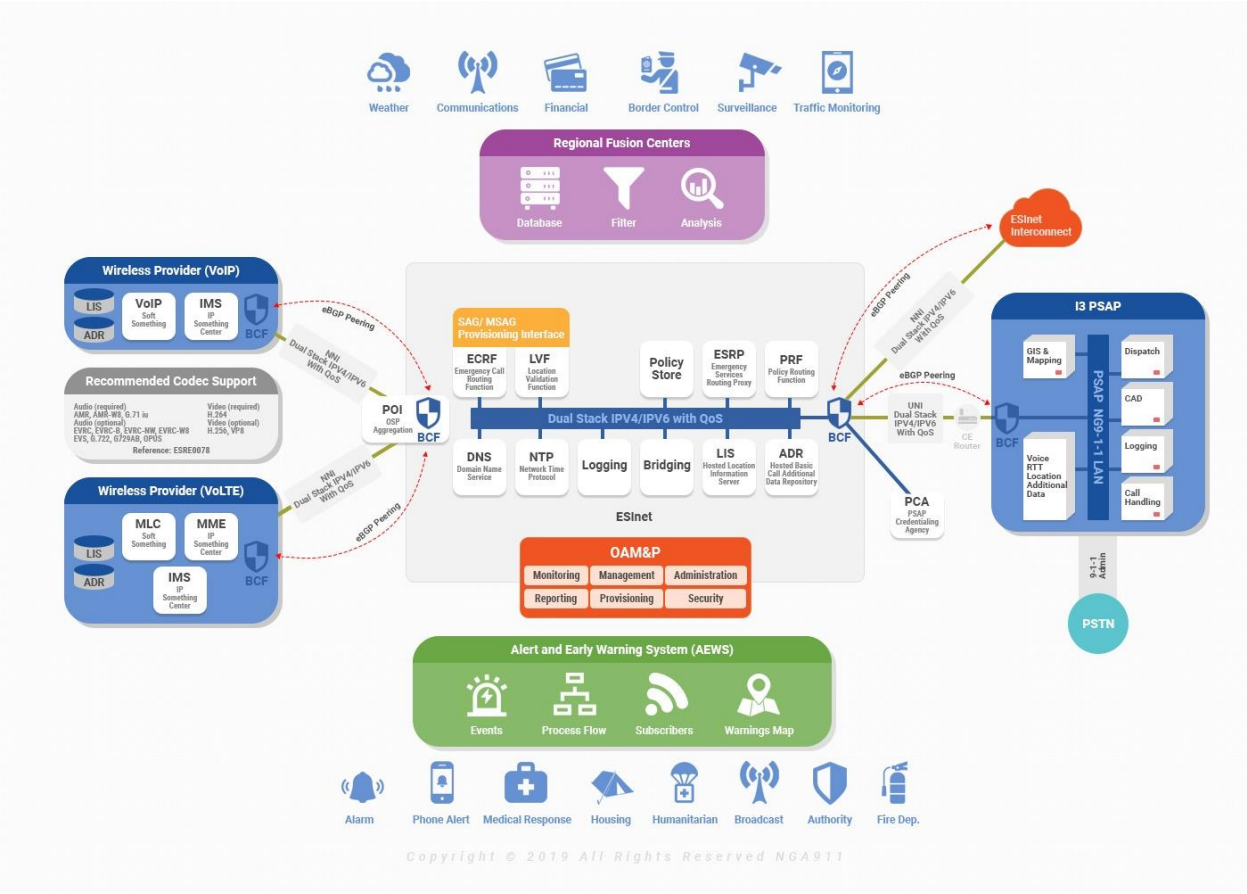
NGA 911's NGCS is fully i3 compliant and can accommodate any media (Text, video, voice) a 911 caller or PSAP is able to use.

C. BIDDER REQUIREMENTS

1. Requirements with Response

a. Configuration Solution

NGA 911 has a complete suite of NGCS elements that is fully NENA i3 compliant. Furthermore, The NGA 911 solution is fully backwards compatible and supports any combination of legacy, E9-1-1, i2, and i3 calls delivered to the system as depicted in our system diagram below:



The NGA 911 NGCS solution is entirely deployed in the cloud for best-in-class availability, reliability and security. The NGCS is exclusively accessed through robust NG9-1-1 specified Border Control Functions (BCF) and secure web-portal proxies. The proposed NGA 911 solution integrates the following NG9-1-1 functional elements:

Legacy Network Gateway (LNG). The LNGs ensure that any legacy calls coming into the NGA 911 core are converted into NENA i3 compliant formats. Until the PSAP is migrated off the legacy Selective Router (SR) NGA 911 will house an LNG at the SR to convert legacy SS7 to SIP while also inserting the available location information into a PIDF-LO format. The LNG through two diverse AWS Direct Connect paths is connected to the NGCS for call processing. The LNG location interworking function (LIF) and network interworking function (NIF) functions are redundantly deployed (>99.999% available) in our Cloud with

protocol interworking function (PIF) deployed at any central office (CO) or tandem in each LATA as required technically or by agreement.

Legacy PSAP Gateway (LPG). During the transition to a fully NENA i3 compliant Next Generation system NGA 911 will supply LPG's for each PSAP that requires legacy support to interoperate with the NGCS. The specific implementation of the LPG at a PSAP is dependent on the legacy CPE deployed. The configuration of the LPG at a PSAP will bring that PSAP into compliance with the ESInet and NG9-1-1 from a technical perspective. Typical variants are:

- Analog (CAMA) trunked with serial ALI
- SIP (non i3) trunked with serial ALI
- SIP (non i3) with IP ALI

Border Control Function (BCF). This element of our solution interfaces our core to the outside world. The NGA 911 solution includes the incorporation and use of BCF as appropriate with security devices implemented in the ESInet and at the "edge" of the proposed CPE. The physical location or the virtual implementation of the BCFs are dependent on the equipment and capabilities of interfacing partners. NGA supplies i3 compliant or custom interfacing options (for non-compliant providers) as follows:

- OSP - BCF
  - i. Direct Cloud Interface (Peering or Transit Gateway)
  - ii. Cross Connect Interface (IXC)
  - iii. Direct Physical Interface
- Other ESInets
  - i. Direct Cloud Interface (Peering or Transit Gateway)
  - ii. Cross Connect Interface (IXC)
  - iii. Direct Physical Interface
- Non-NG Networks
  - i. TDM Gateway (PSTN)
  - ii. Media Gateway
  - iii. SS7/SIGTRAN
  - iv. Cross Connect Interface (IXC)
  - v. Direct Physical Interface
- PSAPs
  - i. Physical Connection with PSAP FW (VPN)
  - ii. Virtual Connection with PSAP BCF
  - iii. Provisioning of BCF for non-compliant PSAPs offered by NGA 911

Emergency Services Routing Proxy (ESRP). The NGA 911 ESRP is located in the cloud and interfaces with the outside world safely through the BCF. The ECRF and the PRF ensure that routing instructions, routing policies and possible

event notifications that alter call routing scenarios are acknowledged. In accordance with NENA STA-010.2-2016 for 9-1-1 calls received in the NGA 911 ESRP first evaluates a policy “rule set” for the queue the call arrives on, then queries the location-based routing function (ECRF) to determine the predefined next hop (smaller political or network subdivision, PSAP or call taker group) Universal Resource Identifier (URI). It will then check with the PRF to see if there are any temporary conditions that will require a different hop.

Policy Routing Function (PRF). The PRF manages information about abandoned PSAP system functionality. Conforming to the NENA i3 standard, the NGA 911 PRF allows PSAPs and Emergency Telephone System Boards (ETSBs) to define “special condition” routing plans for calls/texts in case of unique situations that are outside of normal operations in the PSAPs or on the ESInet (e.g. during maintenance, emergency outage, or manning schedules). The PRF monitors the ESRP’s downstream queues to actively understand each potential entity’s queue status.

Emergency Call Routing Function (ECRF). This element will process 9-1-1 calls and sessions routed with the appropriate (URI) from the ESRP. The ESRP enables the acquisition of a PSAP-routable address by invoking the ECRF. The ECRF will acquire the location by one of two methods. Either by reading a valid address directly embedded inside the call itself or by querying an external data source based on an embedded reference in the call.

Location Validation Function (LVF). The LVF verifies a civic address within an acceptable location reference system like the United States Postal Address. The LVF ensures that the location falls within a range of known values, and that a location is able to be referenced for mapping. The LVF makes no assumption about the association between the caller and the caller's location.

Spatial Interface (SI). The NGA 911 SI enables data updates from our Geographic Information Systems (GIS) solution to the ECRF and LVF. Authorized 9-1-1 entities can also utilize SI services provided by NGA 911 via our secure web-portal to make updates to the LVF and ECRF (e.g. PSAP boundary changes).

Legacy Selective Router Gateway (LSRG). The NGA 911 LSRG facilitates the NGCS to transfer and/or receive calls with Automatic Number Identification (ANI) and Automatic Location Identification (ALI) information to legacy SR. This capability allows the legacy PSAPs and upgraded PSAPs to work seamlessly together within the same NGA 911 Next Generation Core during transition.

Location Database (LDB). The NGA 911 LDB serves as both a legacy ALI database and as a LIS in an i3 NG9-1-1 environment. The LDB will retain all of the current information, functionality, and interfaces of today’s ALI, but also can use the new protocols required in an NG9-1-1 deployment. The LDB supports the

protocols for legacy ALI query and ALI query service, the protocols required to obtain information for wireless calls by querying the mobile positioning center ("MPC") or gateway mobile location center ("GMLC"), and the protocols required for i3 location information retrieval and conveyance, such as HELD or other proprietary protocols. This allows the LVF working in conjunction with the LDB to validate addresses from either legacy MSAG formatted locations or i3 based PIDF-LO formatted ones. NGA 911 discrepancy reports from the LDB conform to Section 4.7 of STA-010.2-2016.

Logging and Recording. The NGA 911 logging service will log NG9-1-1-related events, transactions, media, and operations. Logging includes all elements in the call flow including logging of events within ESInets, the NGCS, the PSAP, and related operations and is a standardized function used throughout ESInets, NG9-1-1 functional elements, and PSAPs. Logged events include ingress and egress to an ESInet, ingress and egress to a PSAP, all steps involved in call processing, and processing of all forms of media.

The NGCS also provides voice, text and media long term recording accessible to the PSAP via the web-portal for recovery and review. These recordings will be saved for a period of time based on the requirements of Alaska, 5 years, 7 years, etc.

b. Attachments

The Cost Proposal has been included with a detailed description of NGA 911's firm fixed pricing.

c. Appendices

NGA 911 has included the following additional documents in the appendices:

- Resumes
- Training Plan
- High-Level Proposed Project Plan
- NENA Security Audit Checklist

d. Brochures

NGA 911 has not provided any additional brochures as an attachment to this RFP.

D. GENERAL REQUIREMENTS - TECHNICAL

1. Commission Requirements

a. Industry Standards

NGA 911 standards based and non-proprietary ESInet solution is in full compliance with all of the standards, requirements, and recommendation located in Table 1: Adopted Standards in section III.D.1 of Nebraska's RFP. Furthermore, our solution is in full compliance with the relevant recommendations and requirements of the following standards:

NENA 08-751, NENA i3 Technical Requirements Document

NENA 04-001, Recommended Generic Standards for E9-1-1 PSAP Equipment

NENA – INF 15.1-2016, NENA NG9-1-1 Security Information Document

NENA 04-503, Network/System Access Security

NENA 75-502, Next Generation Security Audit Checklist

NENA – INF-016.2-2018 (formerly 08-506), Emergency Services IP Network Design for NG9-1-1

NENA 08-752, Location Information to Support IP-Based Emergency Services Requirements

NENA 71-502, An Overview of Policy Rules for Call Routing and Handling in NG9-1-1

NENA-STA-003, NENA Standard for NG9-1-1 Policy Routing Rules

NENA 08-506 Emergency Services IP Network Design for NG9-1-1

Applicable Internet Engineering Task Force Standards (IETF), such as IP protocols, IP routing protocols, SIP, RTP, LoST, and PIDF-LO.

NENA-REQ-002.1-2016, NENA Next Generation 9-1-1 Data Management Requirements

NENA-STA-005.1.1- 2017, NENA Standards for the Provisioning and Maintenance of GIS data to ECRF and LVFs

NENA-STA-006.1-2018, NENA Standard for NG9-1-1 GIS Data Model

NENA-INF-011.1-2014, NENA NG9-1-1 Policy Routing Rules Operations Guide

NENA-STA-012.2-2017 (originally 71-001), NG9-1-1 Additional Data Standard

NENA-INF-023.1-2017, NENA Call Blocking Information Document

NENA-INF-024.2-2018 (originally 04-502), E9-1-1 PSAP Site Characteristics Technical Information Document

NENA-INF-027.1-2018, NENA Information Document for Location Validation Function Consistency

NENA-STA-028.2- 2018 (originally 04- 004), Generic Standards for E9-1-1 PSAP Intelligent Workstation (IWS) Equipment

NENA-INF-029.2-2018 (originally 04-501), Integrating Applications on Intelligent Workstations Technical Information Document

APCO/NENA 2.105.1- 2017, NG9-1-1 Emergency Incident Data Document (EIDD) (ANSI accredited)

NENA 08-501, Interface between the E9-1-1 Service Provider Network and the Internet Protocol (IP) PSAP Information Document

NENA 08-502, E9-1-1 Requirements Information Document

NENA 08-505, Methods for Location Determination to Support IP-Based Emergency Services Information Document

NGA 911 has an in-house R&D team that is constantly improving our solutions. This team not only is responsible for implementing new requirements that come out of the standards body but also actively participating in the NENA standards bodies and consequently tend to be well positioned to quickly implement new requirements or recommendations. NGA 911 will upgrade our NGCS solution in Nebraska well before 18 months after a relevant standard is ratified at no additional cost to the state but as part of our managed services agreement.

As part of our eTOMs and ITIL compliant change management process all updates to the network and their consequences will be submitted to the Commission and its designated public safety stakeholders, who together will comprise the Change Review Board, for approval before any updates or changes are made to the network. No feature will be deprecated without prior approval from the Change Review Board.

b. Public Safety-Grade Definition

NGA 911 understands that the requirements in the four elements that make up their definition of Public Safety-Grade. NGA 911 affirms that its ESInet solution exceeds the minimum requirements of Nebraska definition for Public Safety-Grade. Our NGCS and the processes that support it meet or exceed the national standards listed in Table 1 of in section III.D.1 of Nebraska's RFP.

RFP 6264 Z1

Section IV: Corporate Overview and Technical Approach

Option B

NGA 911

June, 2020

Table of Contents

1) CORPORATE OVERVIEW 2
   a) BIDDER IDENTIFICATION AND INFORMATION 2
   b) FINANCIAL STATEMENTS 2
      i) Description of the Organization 2
      ii) Size of Organization 3
      iii) Longevity 3
      iv) Client Base 3
      v) Areas of Specialization and Expertise 3
      vi) Financial Strength of the Organization 4
      vii) Banking Reference 4
      viii) Judgements and Litigation 4
      ix) Credit Checks 4
   c) CHANGE OF OWNERSHIP 4
   d) OFFICE LOCATION 4
   e) RELATIONSHIP WITH THE STATE 4
   f) BIDDER'S EMPLOYEE RELATIONS TO THE STATE 4
   g) CONTRACT PERFORMANCE 5
   h) SUMMARY OF BIDDER'S CORPORATE EXPERIENCE 5
   i) SUMMARY OF NGA 911'S PROPOSED PERSONEL/MANAGEMENT APPROACH 9
   j) SUMMARY OF NGA 911'S PROPOSED PERSONEL/MANAGEMENT APPROACH 13
2) TECHNICAL APPROACH 13
   a) UNDERSTANDING OF PROJECT REQUIREMENTS 13
   b) PROPOSED DEVELOPMENT APPROACH 23
   c) ATTACHMENT C – TECHNICAL REQUIREMENTS 25
   d) PROPOSED HIGH-LEVEL PROJECT PLAN 26
   e) SCHEDULE FOR THE LIFECYCLE OF THE PROJECT 26
   f) COST PROPOSAL 27

1) CORPORATE OVERVIEW

a) BIDDER IDENTIFICATION AND INFORMATION

Full Company Address	NGA 911, L.LC. 8383 Wilshire Blvd, Suite 800 Beverly Hills, Ca 90211
Entity Organization	Limited Liability Corporation
State in Which Incorporated	California
Year Organized	2016, 5/17/2016
Former Names	NGA 911, Inc

b) FINANCIAL STATEMENTS

i) Description of the Organization

NGA 911 is a privately held company. NGA 911 is a technology company offering advanced Next Generation 9-1-1 (NG9-1-1) services to Public Safety Answering Points (PSAPs). NGA 911 has been offering NG9-1-1 services for more than four years. NGA 911's Next Generation Core Services (NGCS) is a fully compliant National Emergency Number Association (NENA) i3 NG9-1-1 solution. NGA 911's NGCS provides PSAPs with improved resilience, reliability, robustness, cybersecurity, and ultimately access to more call types (real time texting, video, and instant messaging etc.). In a 2019 evaluation of NGCS service providers in California, the California Office of Emergency Services (Cal OES) 9-1-1 Branch awarded their only perfect technical evaluation score to NGA 911 for their regional deployments. This evaluation included i3 compliance, project management capabilities, deployment capabilities, and ongoing support capabilities.

The NGA 911 staff has over 375 combined years in 9-1-1 and over 150 years direct NG9-1-1 experience. Our staff includes two (2) former National NENA Presidents, and current Development Steering Council (DSC) co-chairs of the NENA 9-1-1 Core Services Committee, and the NENA Data Management Standards Committee. We are also active members in APCO and the Industry Council for Emergency Response Technologies (iCERT). In iCERT we co-chair the Emerging Technologies Committee.

As our NGCS is hosted in the Amazon Web Services (AWS) cloud, we have been able to harness the full power of cloud computing by implementing Infrastructure as a Service (IaaS). Our partnership with AWS for IaaS ensures we stay ahead of cyber threats, scales on demand, and employs numerous failover strategies. It enables multiple access points to integrate new technology through innovative collaborative techniques, with no single point of failure. In the

case of 9-1-1 services, this will translate into faster call processing times, increased resource efficiency, quicker response times, and better decision making.

ii) Size of Organization

NGA 911 has 30 employees at the time of the submission of the RFP.

iii) Longevity

NGA 911, L.L.C. was formed on 05/17/2016.

iv) Client Base

NGA 911 has launched our NGCS and ESInet in West Virginia, California, and Elko County, Nevada. NGA 911 has deployed NG9-1-1, including ESInet and CPE capabilities in Elko County, Nevada, and upcoming this month in Logan County, West Virginia.

- NGA 911 is the vendor supporting 50% of California's geographical area under the Cal OES NG9-1-1 Next Gen Network contract representing 189 PSAPs and delivering over 14M 9-1-1 calls per year.

- NGA 911 has deployed an ESInet, NGCS, GIS, and CPE solution in Elko County, NV.

- NGA 911 is also currently involved in 34 Step 1 trials of NGCS in jurisdictions across the United States. These Step 1 trials take a "prove it to me" approach where we route NG 9-1-1 SIP media to the existing PSAP CPE. This provides the PSAP with a practical understanding of where their specific environment, including CPE, stands in reference to migrating to NG9-1-1. It has also built a tremendous body of knowledge within NGA 911 about CPE integration with the NGA 911 NGCS.

v) Areas of Specialization and Expertise

NGA 911 has designed and engineered the spectrum from small scale systems (1 - 3 PSAP in a county) to much larger scale networks (~200 PSAPs in a state). We have installed these same PSAP systems and provided comprehensive support and maintenance to them including network monitoring, continuing training, incident management coordination, change management services, and on-site technician support. Furthermore, NGA 911 is an industry recognized intellectual leader in the NG9-1-1 communications industry. Its employees have been and continue to be deeply involved in supporting the work of the industry's standards committees.

vi) Financial Strength of the Organization

the company to provide its emergency call routing, transport, and related functionalities based upon contracts with state and municipal governmental agencies. Under this plan, our investor's capital will ensure successful deployment of 9-1-1 services in Nebraska and revenue from the continued delivery of those services will be sufficient to continue the operation of those 9-1-1 services.

vii) Banking Reference

Eddie P Coutino | Chase | Branch Manager | NMLS ID 97988 I 102 w Foothill Blvd. Monrovia, CA 91016 T: 626-357-7472 eddie.p.coutino@chase.com |

viii) Judgements and Litigation

No such condition is known to exist.

ix) Credit Checks

NGA understands that the State may elect to use a third party to conduct credit checks as part of the corporate overview.

c) CHANGE OF OWNERSHIP

NGA 911 is a privately held company. NGA 911 does not foresee any change in ownership or control of the company during the 12 months following the proposal due date. NGA 911 understands that any change of ownership will require notification to the State and will comply.

d) OFFICE LOCATION

NGA 911, L.L.C.
8383 Wilshire Blvd, Suite 800
Beverly Hills, CA 90211

e) RELATIONSHIP WITH THE STATE

NGA 911 has had no previous dealings with the State over the previous five years.

f) BIDDER'S EMPLOYEE RELATIONS TO THE STATE

No such termination for default has been experienced by NGA 911 in the past five (5) years.

g) CONTRACT PERFORMANCE

NGA 911 does not employ any personnel that were employees of the State of Nebraska. No such relationship exists.

h) SUMMARY OF BIDDER'S CORPORATE EXPERIENCE

Previous projects similar to this solicitation in size	**Contract No.**	**Scope**	**Complexity**
Los Angeles Region, CA	6061-2019	79 Public Safety Answering Points (PSAPs) migrated to a Regional ESInet and Cloud NGCS.	Coordinating 79 PSAPs to deploy in a Phased approach, this includes coordination of Originating Service Provider (OSP) aggregation provisioning the ESInet, site surveys, remediation, ordering backroom equipment and installation of equipment.
Central Region, CA	6060-2019	114 Public Safety Answering Points (PSAP)s migrated to a Regional ESInet and Cloud NGCS.	Coordinating 114 PSAPs to deploy in a Phased approach, this includes coordination of Originating Service Provider (OSP) aggregation, provisioning the ESInet, site surveys, remediation, ordering backroom equipment and, installation of equipment.
Elko County, NV		Three (3) geodiverse PSAPs. Migrated from Basic 9-1-1 (B9-1-1) to a Next Generation 9-1-1 (NG9-1-1) ESInet and Cloud NGCS.	Elko County is the fourth-largest county by area in the contiguous United States. This project included the migration of OSP traffic to the NGCS, deployment of the ESInet, GIS layers for call routing and deployment of cloud CPE for the cities of Elko and West Wendover NV and the Owyhee Tribal Nation. These three agencies share and are able to transfer calls over the ESInet. and share the hosted CPE.

NARRATIVE DESCRIPTION

- **Number of ESInet and NGCS solutions implemented and are in production today?**

NGA 911 has 4 ESInet and NGCS solutions implemented and are in production today including:

  - California
  - Nevada
  - West Virginia
  - Louisiana

- **Lessons Learned throughout the project that will be applied to Nebraska ESInet and NGCS solution**

NGA 911 has learned several key lessons throughout the project deployments in other states that will be applied to Nebraska. These lessons learned will allow NGA 911 to stay on task and meet critical milestones. Lessons learned include:

Start engaging with ESInet and PSAPs early. The migration onto the new NGCS platform takes several steps and there are necessary milestones to complete the migration from the existing legacy network to the NGA 911 NGCS.

From what we know currently, we believe the best case to have the ESInet interconnected with the trunks tested to be 6-9 months.

We have also provided additional information for your review.

Coordinate with all telecommunications providers and manage circuit order processes to include testing and integration

NGA 911 will coordinate with all telecommunications providers and manage circuit order processes to include testing and integration. NGA 911 will assign a NG Trunk Coordinator. The NG Trunk Coordinator will be responsible for, but not limited to:

- Manage FOC dates with carriers
- Coordinating site walk throughs (if requested by provider)
- Coordinating Installation and Testing
- Coordinating Integration and System Testing
- Communication with the NGA 911 Project Manager to provide status of circuit order and installation

Los Angeles Region, CA

Time Period of Project	Start Date: 8/20/2019 End Date: 8/19/2024
Scheduled and Actual Completion Dates	Scheduled: 1/2021 Actual: On Going
Bidder's Responsibilities	NGA 911 is implementing, managing, and overseeing an ESInet and cloud based NGCS for 80 PSAPs. NGA 911 will aggregate, process and deliver all 9-1-1 traffic from AT&T, Consolidated Communications wireline and Frontier wireline, and all wireless Originating Service Providers (OSPs) to the correct PSAP.
Reference	Budge Currier Branch Manager Budge.Currier@caloes.ca.gov (916) 657-9911
Prime Contractor or Subcontractor Scheduled Completion Date Budget Currently Planned Completion Date Currently Planned Budget	NGA 911 is Prime Contractor 1/2021 $54,281,000.00 1/2021 or earlier $54,281,000.00

Central Region, CA

Time Period of Project	Start Date: 8/20/2019 End Date: 8/19/2024
Scheduled and Actual Completion Dates	Scheduled: 1/2021 Actual: On Going
Bidder's Responsibilities	NGA 911 is implementing, managing, and overseeing an ESInet and cloud based NGCS for 111 PSAPs. NGA 911 will aggregate, process and deliver all 9-1-1 traffic from AT&T, Consolidated Communications wireline and Frontier wireline, and all wireless Originating Service Providers (OSPs) to the correct PSAP.
Reference	Budge Currier

	Branch Manager Budge.Currier@caloes.ca.gov (916) 657-9911
Prime Contractor or Subcontractor Scheduled Completion Date Budget Currently Planned Completion Date Currently Planned Budget	NGA 911 is Prime Contractor 1/2021 $54,281,000.00 1/2021 or earlier $54,281,000.00

Elko County, NV

Time Period of Project	Start Date: 6/12/2019 End Date: 6/12/2024
Scheduled and Actual Completion Dates	Scheduled: 8/2020 Actual: 5/2020 Elko County PD (CDAA): 5/20/2020 West Wendover PD: 5/22/2020 Owyhee Tribal Nation: Pending. This PSAP is building a new building and install will be scheduled upon completion of build.
Bidder's Responsibilities	NGA 911 is implementing, managing, and overseeing an ESInet and cloud based NGCS for 3 PSAPs. NGA 911 will aggregate, process and deliver all 9-1-1 traffic from wireless, wireline, VoIP traffic. Additionally, this project included GIS and CPE with Text to 9-1-1.
Reference	Cash Minor Assistant County Manager/CFO cminor@elkocountynv.net (775) 753-7073
Prime Contractor or Subcontractor Scheduled Completion Date Budget Currently Planned Completion Date Currently Planned Budget	NGA 911 is Prime Contractor 8/2020 $1,147,611.33 5/22/2020 $1,147,611.33

i) SUMMARY OF NGA 911'S PROPOSED PERSONEL/MANAGEMENT APPROACH

Approach to Management of Project

Throughout the course of the NGCS Project NGA 911 will provide professional services to the State of Nebraska to effectively design and implement the new system as well as smoothly integrate its capabilities into the State's emergency communications processes. These services will be organized around three phases:

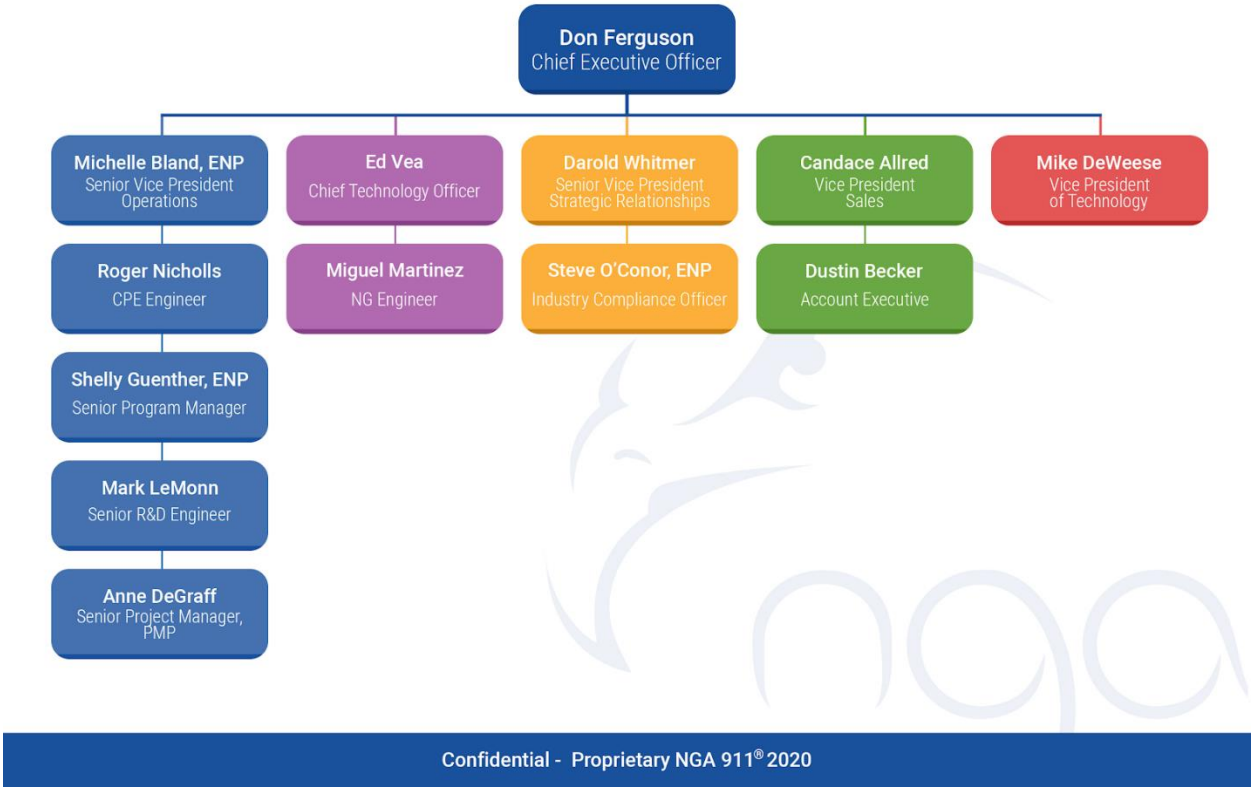
Solution Planning. During this phase NGA 911 will collect all the necessary requirements for the project and catalog the needs and constraints of each of the primary and secondary PSAP locations. NGA 911 and the Commission together will agree on the final scope of the project; NGA 911 will document that scope in a master plan which will include a master schedule, a trunk provisioning plan, an ESInet Interface plan, and a PSAP equipment inventory plan and PSAP LAN wiring plan to connect all of the PSAPs to the ESInet.

Solution Implementation. In this phase NGA 911 will order, implement, test, validate and accept all the NG trunks required for the ESInet connections to the NG Core as well as the networking hardware required at the Data Centers to actualize the ESInet and the hardware required to support the ESInet and each of the PSAPs. We will dimension the cloud platform and establish a dedicated instance for the State of Nebraska of the NGCS capabilities. We will implement, test and validate the performance of the ESInet interfaces. We will also connect the NOC to all of the solution elements as they are turned and begin monitoring the system.

Solution Testing and Cutover. Once all the solution elements are installed and validated at for each PSAP location we will perform rigorous end to end acceptance testing. Once the system passes each of the thresholds in the test plan the system will be ready for cutover and to begin operation. As part of the preparation for going live PSAP and Commission personnel will be trained on the new systems during this testing and cutover phase.

All of the services required to complete the tasks listed above will be provided by NGA 911 and reflected as a onetime cost for the initial implementation of our proposed next generation emergency communications system. More details on the cost and timeline for the implementation of these services can be found in the Proposed High-Level Project Plan and Section: Schedule for Life Cycle of the Project. All personnel belonging to NGA 911, who will be working in the State's PSAP locations will be CJIS cleared with the proper documentation submitted to the proper PSAP authority at least 5 days prior to their first visit. NGA 911 understands that all personnel must be properly cleared and badged before doing any work in a PSAP and furthermore will abide by any other security requirements that currently exist or may be implemented in the future at any PSAP location in the State of Nebraska.

NGA 911 Leadership



Personnel Assigned to Nebraska Project

NGA 911 resumes have been included as an attachment.

Role	Name	Experience	Responsibility
Executive Sponsor	Candace Allred	20 years serving the 9-1-1 Public Safety Community in delivering mission critical solutions and services. Mrs. Allred has a passion for ensuring tools delivered support both	Ms. Allred is responsible for financially authorizing the project and creating the project charter. Ms. Allred will work closely with the project manager (PM). Ms. Allred is accountable to the board: Owns the business case. Keeps the project aligned with the organization's strategy and portfolio direction. She will govern project risk and work with other sponsors.

		the health and wellness of first responders in the 9-1-1 Industry.	
Project Manage ment and Oversight	Michelle Bland	16 years in the 9-1-1 industry with an additional 13 years in telecom. Ms. Bland is an ENP and a CMCP. Approximately 3 years with NG9-1-1 deployments. Ms. Bland holds A Bachelor's Degree in Accounting and a Master's Degree in Global Business Management.	Ms. Bland will oversee the project as the project director to ensure all tasks are completed. Additionally, Ms. Bland will be your first point of contact for any issues that cannot be resolved by the Project Manager. Ms. Bland was the 9-1-1 Program Manager for the California Highway Patrol for over 10 years. In this position she oversaw 25 communications centers which included troubleshooting, CPE procurement and deployment, building moves, furniture installation, analytic reporting, and administering the wireless program.
Project Manager, PMP	Anne DeGraff	Over 40 years in the computing and communications fields with over 25 years managing complex technical as well as Public Safety projects	Ms. DeGraff's experience includes over 40 years in the computing and communication fields with over twenty-five years managing complex technical as well as Public Safety projects – Qwest/CenturyLink, Intrado/West Safety Services. Excels in organizing, planning, scheduling and successfully delivering on challenging multi PSAP and vendor deployments. Expertise in Program Management, Project Management, Customer Relations, Strategic Planning and Execution as well as Team Building.
Project Manager	Shelly Guenther	26 years in the 9-1-1 industry, 15 years in NG9-1-1 as an NG9-1-1 Product and Project Manager. Ms. Guenther is an ENP and is the NENA DSC Data Management Co-Chair	Ms. Guenther has been in project management throughout her career. Ms. Guenther is a recognized leader throughout the telecom industry. As a Project Manager for NGA 911, Ms. Guenther successfully deployed Elko County, NV consisting of 3 PSAPs which transitioned from basic 9-1-1 to NG9-1-1 with a CPE upgrade and GIS component. She also supported both the Logan County, WV and California NG9-1-1 deployments. Ms. Guenter has experience working directly with the PSAP to ensure all tasks, milestones are met on time and continued constant communication is had with the PSAP and Stakeholders.

NG9-1-1 Trunk Services Coordinator	Miguel Martinez	25 years supporting the 9-1-1 industry including CPE and network connectivity. Approximately 3 years supporting ESInet and NGCS deployment for NG9-1-1.	Primary role will be evaluating the NG Trunks to support State of Nebraska PSAPs. Mr. Martinez will procure and ensure timely installation. Mr. Martinez has been in the 9-1-1 industry for more than 25 years. He has been supporting the PSAP installations and has a superior knowledge of PSAP backrooms, CPE, and connectivity requirements.
CPE Engineer	Roger Nicholls	Over 35 years in CPE installation, maintenance and support for the 9-1-1 industry.	Lead PSAP backroom Engineer. Mr. Nicholls worked as the lead service technician for Frontier Communications and Verizon for more than 20 years. He has installed and maintained CPE systems for various 9-1-1 CPE platforms.
NG9-1-1 Aggregation Services Coordinator	Mike DeWeese	29 years in the 9-1-1 industry, 15 years' experience NG9-1-1	Mr. DeWeese will coordinate OSP aggregation and network cutover plans. Mr. DeWeese has worked with OSPs and the buildout of NG9-1-1 networks for more than 20 years.
NGCS Engineer	Ed Vea	30 years in telecommunications and 18 in Public Safety technical roles	Ed Vea is NGA 911's Chief Technology Officer and lead NG9-1-1 core services engineer
Network Engineer and NOC	Mark LeMonn	15 years in IT Management with 8 years in 9-1-1 and an additional 2 years supporting NG9-1-1 projects.	Responsible for network monitoring, outage reporting, troubleshooting, liaison with NOC/SOC. Mr. LeMonn has worked in IT and troubleshooting for PSAPs for more than 10 years.

<u>Additional Leadership Experience:</u>

Chief Executive Officer - Don Ferguson

- 30 years in the industry, 5 years in NG9-1-1

Senior Vice President, Strategic Relationships – Darold Whitmer

- 28 years in the industry, 15 years in NG9-1-1 and a total of 46 years in data and telecom. Mr. Whitmer was the Executive Sponsor of the only successful USDoT funded NG9-1-1 trial in 2010 to 2012. The trial was the NE California Locate Before Route project.

Chief Compliance Officer – Steve O'Conor, ENP

- 46 years in the industry, 18 years in NG9-1-1 as a NG9-1-1 Industry Compliance Officer, on the National Emergency Number Association (NENA) Development Steering Committee (DSC) as Co-Chair in various roles

Chief Financial Officer /Treasurer - Ishka Villa

- 11 years in the industry

j) SUMMARY OF NGA 911'S PROPOSED PERSONEL/MANAGEMENT APPROACH

NGA 911 does not intend to use subcontractors as a part of this contract.

2) TECHNICAL APPROACH

a) UNDERSTANDING OF PROJECT REQUIREMENTS

Products and Services

All NGA 911 ESInet and NGCS software is 100% deployed in the cloud, providing the best possible reliability and availability in the industry. All functional elements (FE) of the NGA 911 NGCS are designed, architected and deployed on the AWS Cloud in a manner which strictly adheres to the criteria defined in NENA-STA-010.2-2016 for an NGCS.

All Amazon Web Services (AWS) data centers and direct connect facilities are designed to an Uptime Institute level of Tier III+ or above. The NGA 911 solution is fully redundant, deploys dual Cores in four (4) Availability Zones (AZ) for a total of eight (8) Cores. The AWS AZs are required to be a minimum of 10 miles apart and on separate power grids. The AZs are connected by multiple high-speed broadband carriers in meshed networks. Having eight (8) cores allows NGA 911 to exceed the State of Nebraska's five 9s availability requirement.

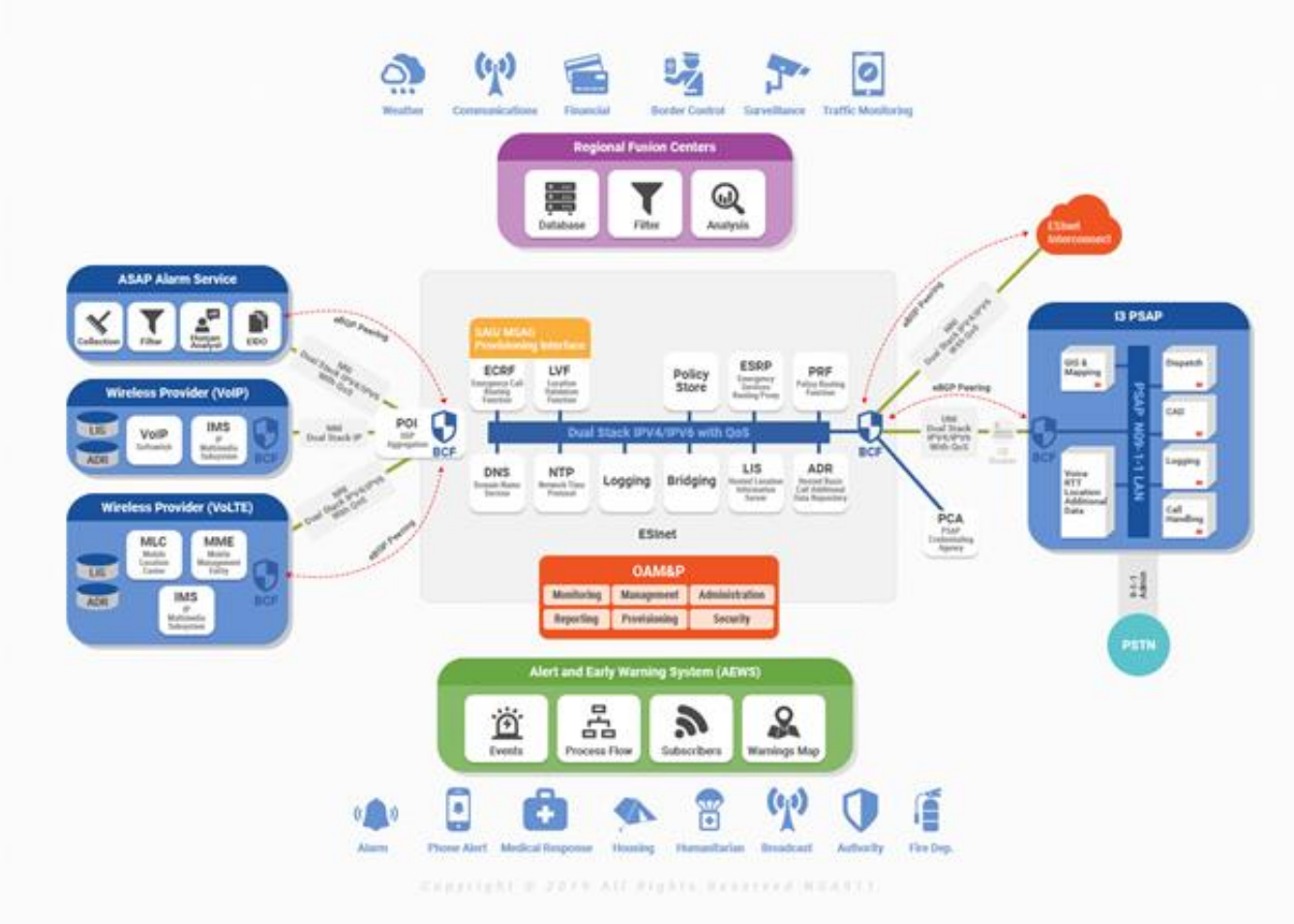
NGCS	Non Redundant 1 AZ		Redundant 2 AZ		Redundant Region 2 AZ's each	
Functional Element	**Signaling**	**Media**	**Signaling**	**Media**	**Signaling**	**Media**
Aggregation Point	99.90%	99.95%	= 5 9's	> 5 9's	100.00%	100.00%
NG911 Trunk	99.99%	99.99%	> 5 9's	> 5 9's	100.00%	100.00%
BCF	99.99%	99.99%	> 5 9's	> 5 9's	100.00%	100.00%
NGCS	99.84%	99.95%	> 5 9's	> 5 9's	100.00%	100.00%
BCF	99.99%	99.99%	> 5 9's	> 5 9's	100.00%	100.00%
NG911 Trunk	99.99%	99.99%	> 5 9's	> 5 9's	100.00%	100.00%
@ PSAP/CPE	**99.70%**	**99.86%**	**= 5 9's**	**> 5 9's**	**> 5 9's**	**> 5 9's**

**100% signifies many 9's above five 9's*

Each of the eight (8) NGCS cores is architected to support 100% of the traffic for the State of Nebraska. The NGA 911 cores operate in an active-active mode. SIP Signaling is processed through the eight (8) cores dedicated to the State of Nebraska utilizing a load balancing round robin approach that ensures all network FE's are constantly and consistently exercised. In the event of failure of any one stack, that supporting core infrastructure is taken offline and replaced with a new container of the instance without effect to the other operational cores. This approach ensures that there is never a gap in availability and exceeds the five 9s requirements defined by the State of Nebraska. 100% of the platform capacity will survive any single element of the solution experiencing a failure.

NGCS

NGA 911 has a complete suite of NGCS elements that is fully NENA i3 compliant. Furthermore, The NGA 911 solution is fully backwards compatible and supports any combination of legacy, E9-1-1, i2, and i3 calls delivered to the system as depicted in our system diagram below:



The NGA 911 NGCS solution is entirely deployed in the cloud for best-in-class availability, reliability and security. The NGCS is exclusively accessed through robust NG9-1-1 specified Border Control Functions (BCF) and secure web-portal proxies. The proposed NGA 911 solution integrates the following NG9-1-1 functional elements:

Legacy Network Gateway (LNG). The LNGs ensure that any legacy calls coming into the NGA 911 core are converted into NENA i3 compliant formats. Until the PSAP is migrated off the legacy Selective Router (SR) NGA 911 will house an LNG at the SR to convert legacy SS7 to SIP while also inserting the available location information into a PIDF-LO format. The LNG through two diverse AWS Direct Connect paths is connected to the NGCS for call processing. The LNG location interworking function (LIF) and network interworking function (NIF) functions are redundantly deployed (>99.999% available) in our Cloud with protocol interworking function (PIF) deployed at any central office (CO) or tandem in each LATA as required technically or by agreement.

Legacy PSAP Gateway (LPG). During the transition to a fully NENA i3 compliant Next Generation system NGA 911 will supply LPG's for each PSAP that requires legacy support to interoperate with the NGCS. The specific implementation of the LPG at a PSAP is dependent on the legacy CPE deployed. The configuration of the LPG at a PSAP will bring that PSAP into compliance with the ESInet and NG9-1-1 from a technical perspective. Typical variants are:

- a. Analog (CAMA) trunked with serial ALI
- b. SIP (non i3) trunked with serial ALI
- c. SIP (non i3) with IP ALI

Border Control Function (BCF). This element of our solution interfaces our core to the outside world. The NGA 911 solution includes the incorporation and use of BCF as appropriate with security devices implemented in the ESInet and NGCS. The physical location or the virtual implementation of the BCFs are dependent on the equipment and capabilities of interfacing partners. NGA supplies i3 compliant or custom interfacing options (for non-compliant providers) as follows:

- a. OSP - BCF
    - i. Direct Cloud Interface (Peering or Transit Gateway)
    - ii. Cross Connect Interface (IXC)
    - iii. Direct Physical Interface
- b. Other ESInets
    - i. Direct Cloud Interface (Peering or Transit Gateway)
    - ii. Cross Connect Interface (IXC)
    - iii. Direct Physical Interface
- c. Non-NG Networks
    - i. TDM Gateway (PSTN)
    - ii. Media Gateway
    - iii. SS7/SIGTRAN
    - iv. Cross Connect Interface (IXC)
    - v. Direct Physical Interface
- d. PSAPs
    - i. Physical Connection with PSAP FW (VPN)
    - ii. Virtual Connection with PSAP BCF
    - iii. Provisioning of BCF for non-compliant PSAPs offered by NGA 911

Emergency Services Routing Proxy (ESRP). The NGA 911 ESRP is located in the cloud and interfaces with the outside world safely through the BCF. The ECRF and the PRF ensure that routing instructions, routing policies and possible event notifications that alter call routing scenarios are acknowledged. In accordance with NENA STA-010.2-2016 for 9-1-1 calls received in the NGA 911 ESRP first evaluates a policy "rule set" for the queue the call arrives on, then queries the location-based routing function (ECRF) to determine the predefined next hop (smaller political or network subdivision,

PSAP or call taker group) Universal Resource Identifier (URI). It will then check with the PRF to see if there are any temporary conditions that will require a different hop.

Policy Routing Function (PRF). The PRF manages information about abandoned PSAP system functionality. Conforming to the NENA i3 standard, the NGA 911 PRF allows PSAPs and Emergency Telephone System Boards (ETSBs) to define “special condition” routing plans for calls/texts in case of unique situations that are outside of normal operations in the PSAPs or on the ESInet (e.g. during maintenance, emergency outage, or manning schedules). The PRF monitors the ESRP’s downstream queues to actively understand each potential entity’s queue status.

Emergency Call Routing Function (ECRF). This element will process 9-1-1 calls and sessions routed with the appropriate (URI) from the ESRP. The ESRP enables the acquisition of a PSAP-routable address by invoking the ECRF. The ECRF will acquire the location by one of two methods. Either by reading a valid address directly embedded inside the call itself or by querying an external data source based on an embedded reference in the call.

Location Validation Function (LVF). The LVF verifies a civic address within an acceptable location reference system like the United States Postal Address. The LVF ensures that the location falls within a range of known values, and that a location is able to be referenced for mapping. The LVF makes no assumption about the association between the caller and the caller's location.

Spatial Interface (SI). The NGA 911 SI enables data updates from the State of Nebraska’s Geographic Information Systems (GIS) data provider to the ECRF and LVF. Authorized 9-1-1 entities can also utilize SI services provided by NGA 911 via our secure web-portal to make updates to the LVF and ECRF (e.g. PSAP boundary changes).

Legacy Selective Router Gateway (LSRG). The NGA 911 LSRG facilitates the NGCS to transfer and/or receive calls with Automatic Number Identification (ANI) and Automatic Location Identification (ALI) information to legacy SR. This capability allows the legacy PSAPs and upgraded PSAPs to work seamlessly together within the same NGA 911 Next Generation Core during transition.

Location Database (LDB). The NGA 911 LDB serves as both a legacy ALI database and as a LIS in an i3 NG9-1-1 environment. The LDB will retain all of the current information, functionality, and interfaces of today’s ALI, but also can use the new protocols required in an NG9-1-1 deployment. The LDB supports the protocols for legacy ALI query and ALI query service, the protocols required to obtain information for wireless calls by querying the mobile positioning center (“MPC”) or gateway mobile location center (“GMLC”), and the protocols required for i3 location information retrieval and conveyance, such as HELD or other proprietary protocols. This allows the LVF working in conjunction with the LDB to validate addresses from either legacy MSAG

formatted locations or i3 based PIDF-LO formatted ones. NGA 911 discrepancy reports from the LDB conform to Section 4.7 of STA-010.2-2016.

Logging and Recording. The NGA 911 logging service will log NG9-1-1-related events, transactions, media, and operations. Logging includes all elements in the call flow including logging of events within ESInet, the NGCS, the PSAP, and related operations and is a standardized function used throughout ESInet, NG9-1-1 functional elements, and PSAPs. Logged events include ingress and egress to an ESInet, ingress and egress to a PSAP, all steps involved in call processing, and processing of all forms of media.

The NGCS also provides voice, text and media long term recording accessible to the PSAP via the web-portal for recovery and review. These recordings will be saved for a period of time based on the requirements of the State of Nebraska.

Time Server. The NGA 911 solution provides redundant, resilient network-attached time sources (master clocks) capable of supplying standard time to all systems, network devices, and functional elements that comprise the ESInet and the NGCS that provide accurate timing with no more than 20 milliseconds (ms) of drift from real time between any device(s). System timing is a critical issue for accurate logging across diverse systems. NGA 911's Time Sync Service is fully compliant with the NENA Detailed Functional and Interface Standards for the NENA i3 Solution NENA-STA-010 sections 5.2.2.7 and 5.3.2.4.

Licenses, Subscriptions, and Professional Services

1) The NGA 911 solution is a managed service and does not have any license restrictions.
2) The NGA 911 solution does not have any recurring services for subscription or hosting. This is a managed service and all software, accesses, functionality and hosting are included in the overall cost of the project and the monthly service fee.
3) All NGA 911 One-time Professional Services are included in the overall cost of the project.

Monitoring, Support, Maintenance, and Warranty Plans

Whether the State of Nebraska awards the ESInet, NGCS, or both to NGA 911, the Commission and the PSAPs can be assured that all elements of the NGA 911 solutions from the NGCS through the ESInet to the Cloud platform are monitored 24x7x365 by our NOC. This monitoring is the foundation of our maintenance approach. Besides monitoring the performance of the solution elements, the NOC also schedules and coordinates all of the proactive maintenance, handles field incident reports from customers, manages and coordinates the resolution process, manages the escalation process, provides real time communications and updates to stakeholders and

dispatches field technicians for onsite repairs and maintenance. Helping to guarantee the best possible network performance, all of our network management procedures are ITIL and eTOMS compliant which ensures that the State of Nebraska's emergency communications systems are managed according to the telecoms industry's best practices.

Scheduled Proactive Maintenance. The preferred maintenance windows for its facilities will be identified and approved by the Commission/PSAPs prior to commencing any work on the components, equipment or network. The NOC will be the primary method for the Commission/PSAPs to interface to NGA 911 during scheduled maintenance and will be required to provide regular updates to the selected Commission/PSAP representative. During scheduled maintenance activities the network and systems will not experience a degradation or disruption of service. Individual components may be taken down for maintenance if an alternate route or redundant system is used to minimize the effect.

Change Management. The NGA 911 solution includes any and all updates and/or upgrades and/or replacements provided through the life of the systems to ensure that all of the State of Nebraska's NGA 911 installation software (including operating systems) is operating on the latest version. NGA 911's customer relationship manager will communicate updates and/or hardware requirements in advance of any version changes. This will include a complete set of documentation on the new capabilities delivered to the State of Nebraska at least 45 days before installation of the new version. Part of this process will include coordinating and scheduling any additional training required to make use of the new version. All version changes and upgrades to any of our hardware or software elements are designed and executed under an ITIL and eTOMS compliant change management process that limits risk to operational performance. This process includes a robust testing protocol and rapid roll back capabilities.

NGA 911 will provide monthly reports detailing change tickets, opened, pending, resolved, and closed. The NGA 911 change management system provides the Commission's program manager and any other identified Stakeholder the ability to review proposed change requests and approve the proposed changes.

Incident Management. NGA 911 will provide 24x7x365 maintenance/technical support for the life of the contract. The State of Nebraska's Commission and PSAPs will receive Help Desk and technical services support for all products and services included in NGA 911's proposed solution. The State of Nebraska's authorities can report network, equipment or software outages and problems to the NOC at any time either by direct phone access or through the NGA 911 web portal. NGA 911's portal provides the State of Nebraska's Commission and PSAP personnel access to ticketing system, a knowledge base, a reporting function, measurement analytics, a monitoring function,

and process automation tools. The NGA 911 NOC responds to incidents based on their severity levels with predefined protocols for escalation, prioritization, and reporting.

Rank and SLA	Level 1 Critical	Level 2 Major	Level 3 Minor	Level 4 Standard
Response/ Acknowledge	< 15 minutes	< 30 minutes	8 hours	Based on request
Tech on Site (if required)	0-2 hours	2 hours	Next Business Day	Based on request
Escalation Threshold	1 hour	2 hours	48 hours	As needed
Communication Objective	Hourly	Every 2 hours	Daily	As needed

Severity Level Definitions:

Severity Level 1: Critical Issue

Definition: A widespread system or application failure. An event or outage that impact 9-1-1 services.

Severity Level 2: Major Issue

Definition: The majority of system/application is in failure.

- Loss of service to less than 25% of the users at a given site, multiple sites, enterprise, or of a given functional area.
- There is a negative impact to activities, yet the error does not impair essential operations. Processing can continue in a restricted manner.
- An event or outage that may impact 9-1-1 services

Severity Level 3: Minor Issue

Definition: Customer is experiencing a partial system or application interruption.

- Customer and operational impacts are low.
- Not impacting the delivery of 9-1-1 calls.

Severity Level 4: Standard Requests

Priority is set as a Four (4)

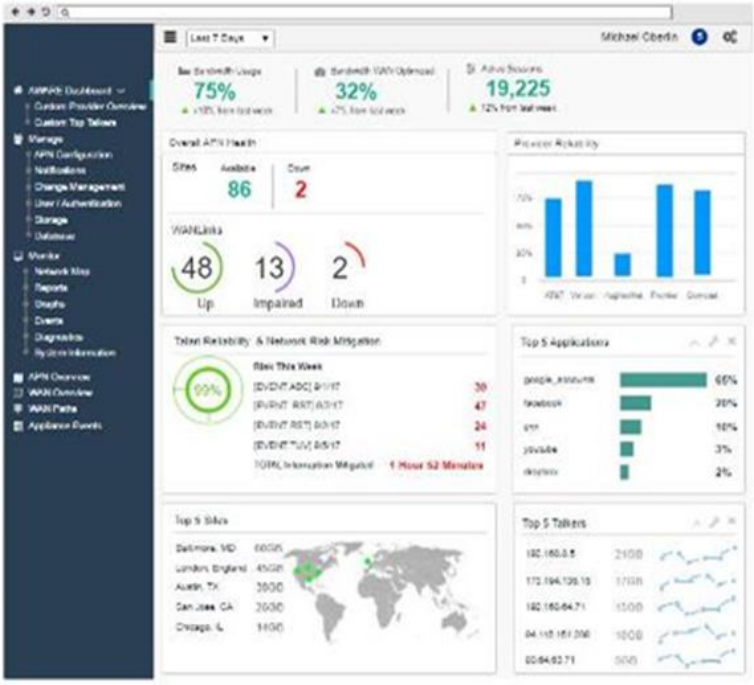
Definition: Not service impacting, yet a potential system/application failure could occur if not resolved.

Visibility and Access to Services

Access to the maintenance services is through the Incident Management System (IMS) which can be accessed by phone or through the NGA 911 Web-Portal.

Reporting and Communications

The NOC will provide monthly reports detailing the performance, changes, incidents, and SLA compliance of the NGA 911 solution. In addition to this formal reporting, authorized personnel from the State of Nebraska's Commission, PSAPs, and any other approved Stakeholder can access the NGA 911 web portal anytime to view reports and dashboards that detail the current and historical status of all of the solution elements. A screenshot of the web portal is below:



Standard Compliance

NGA 911 currently is compliant with NENA, ATIS, 3GPP2, and IETF standards that fully cover the end to end operation of an i3 NG9-1-1 Network, the ESInet, and interfacing with legacy and NG OSPs. NGA 911 will continue to comply with standards as they are

made available. Furthermore, we can quickly develop an interface module for any connection protocol. A list of standards that NGA is currently is compliant with includes, but not limited to:

- NENA-STA-010.2-2016 (formerly NENA 08-003), Detailed Functional and Interface Specification for the NENA i3 Solution, NENA 08-002, NENA Functional and Interface Standards for Next Generation 911 Version 1.0 (i3)
- NENA 08-751, NENA i3 Technical Requirements Document
- NENA 04-001, Recommended Generic Standards for E911 PSAP Equipment
- NENA 75-001, Security for Next Generation 911 Standard (NG-SEC)
- NENA – INF 15.1-2016, NENA NG911 Security Information Document. NENA 04-503, Network/System Access Security
- NENA 75-502, Next Generation Security Audit Checklist
- NENA – INF-016.2-2018 (formerly 08-506), Emergency Services IP Network Design for NG911
- NENA 08-752, Location Information to Support IP-Based Emergency Services Requirements. NENA 71-502, An Overview of Policy Rules for Call Routing and Handling in NG911
- NENA-STA-003, NENA Standard for NG911 Policy Routing Rules
- NENA 08-506 Emergency Services IP Network Design for NG9-1-1
- Applicable Internet Engineering Task Force Standards (IETF), such as IP protocols, IP routing protocols, SIP, RTP, LoST, and PIDF-LO
- Additional Standards and guidelines NGA 911 adhere to:

    - NENA-REQ-002.1-2016, NENA Next Generation 9-1-1 Data Management Requirements.
    - NENA-REQ-001.1.2-2018 Next Generation 9-1-1 PSAP Requirements
    - NENA-STA-005.1.1- 2017, NENA Standards for the Provisioning and Maintenance of GIS data to ECRF and LVFs
    - NENA-STA-006.1-2018, NENA Standard for NG9-1-1 GIS Data Model.
    - NENA-INF-011.1-2014, NENA NG9-1-1 Policy Routing Rules Operations Guide. NENA-STA-012.2-2017 (originally 71-001), NG9-1-1 Additional Data Standard.
    - NENA-INF-015.1-2016, NENA NG911 Security Information Document.
    - NENA STA-015.10-2018 (Originally 02-010), NENA Standard Data Formats for E9 1 1 Data Exchange & GIS Mapping. NENA-INF-023.1-2017, NENA Call Blocking Information Document.
    - NENA-INF-024.2-2018 (originally 04-502), E9-1-1 PSAP Site Characteristics Technical Information Document.
    - NENA-INF-027.1-2018, NENA Information Document for Location Validation Function Consistency.
    - NENA-STA-028.2- 2018 (originally 04- 004), Generic Standards for E9-1-1 PSAP Intelligent Workstation (IWS) Equipment.
    - NENA-INF-029.2-2018 (originally 04-501), Integrating Applications on Intelligent Workstations Technical Information Document.

- APCO/NENA 2.105.1- 2017, NG9-1-1 Emergency Incident Data Document (EIDD) (ANSI accredited).
- NENA 08-501, Interface between the E9-1-1 Service Provider Network and the Internet Protocol (IP) PSAP Information Document.
- NENA 08-502, E9-1-1 Requirements Information Document. NENA 08-505, Methods for Location Determination to Support IP-Based Emergency Services Information Document.
- DOJ CJISD-ITS-DOC-08140-5.6 Criminal Justice Information Services (CJIS) Security Policy
- NIST FIPS 140-33 Security Requirements for Cryptographic Modules
- NENA STA-008.2-2014 Registry System Standard
- NENA INF-016.2-2018 Emergency Services IP Network Design for NG911 (ESIND)
- NERC CIP 002-CIP 009 Critical Infrastructure Protection
- NIST Cybersecurity Framework
- TIA TIA-942-A Telecommunications Infrastructure Standard for Data Centers

Data Centers and Geographic Diversity

Our AWS powered cloud platform is made up of multiple data centers clustered in availability zones (AZ). Our solution will be hosted in two separate regions, one on the east coast and one on the west; it will be further hosted in two different geographically separated AZs within each region.

b) PROPOSED DEVELOPMENT APPROACH

NGA 911's cloud together with our SD-WAN enabled ESInet provides a highly reliable and secure platform that exceeds the State of Nebraska's uptime requirement of 99.999%. This robust platform is the host for our ESInet and NGCS that provide the most advanced emergency 9-1-1 communications capabilities. Both fully conform to the latest NENA i3 standards and are backwards compatible with any legacy needs of the OSPs and your PSAPs. Furthermore, NGA 911 is continuously improving its software to keep pace with the evolving i3 standards, as well as introducing new features that provide improved capabilities to boost the efficiency and accuracy of your PSAPs performance. The solution performance can be monitored in real time through NGA 911's dashboards which are accessed through our web portal.

R&D Approach

At NGA 911, R&D is an integral part of the company mission. Our developers are full time employees. Because our own R&D is in-house, we can quickly adapt our development priorities to meet the needs of our customers. NGA 911 will upgrade our systems to meet new NENA i3 standards within six months of issuance and approval. Before implementing an upgrade on the State of Nebraska's NGCS, we will work with the State to determine the benefits and drawbacks of the particular

upgrades and if the State desires the features. This continuous cycle of improvements and releases are available to the State as part of their services. There is no additional charge for new features.

Technology Evolution Approach

Our NGCS software is regularly patched and/or upgraded to keep it secure, provide advanced features, expand capabilities, implement routine code maintenance and fix bugs. The frequency of scheduled software releases depends on the systems involved. Standards-based functional elements (FE) are not subject to software changes and upgrades and are only modified when new standards are adopted, tested, and then implemented. Software that supports features, services, and functions that are either undefined in the standard or permitted to be customized are regularly updated and modified in accordance with our ITIL and eTOMs compliant change management processes.

NGA 911 uses structured feature release testing and prioritization processes to determine which features and bug fixes to include in each scheduled release. NGA 911 will provide documentation of release notes to the State of Nebraska a minimum of 45 days before implementation. This documentation will detail the deployment process and timeline for all, scheduled and maintenance, releases. In addition, the documentation will describe how NGCS and SD-WAN software releases will be tested and integrated into the NGCS.

Support & Maintenance Approach

The cornerstone of the NGA 911 approach to maintenance is our 24x7x365 managed NOC. The NOC monitors all aspects of the ESInet including our interfaces with the OSPs, as well as the performance of the virtual private clouds that are running the NGCS software. The NGA 911 NOC is operational 24x7x365. The NOC handles coordination (critically, with the PSAPs) for all the communications for both proactive and reactive maintenance that is required on our systems.

In addition, the NOC monitors the performance of our solution's equipment in the PSAPs, this includes the networking equipment for the ESInet. In case of a critical fault in any PSAP-based NGA 911 equipment the NOC will dispatch a field force technician to replace the affected equipment within two hours. NGA 911 will have a local maintenance and support team that is dedicated for the entire contract term.

System Design Approach

Although the NGA 911 solution is designed to use digital VoIP signaling it is fully compatible with legacy analog circuits. If there is a need, during the transition to a NENA i3 end-state, our solution can accommodate existing CAMA circuits for emergency calls. The system uses cost-effective gateway devices to convert the

analog signaling from the CAMA to digital signaling of the IP PBX. Using SIP gateways, the system can easily be configured to accommodate any existing POTS, T1, or ISDN/PRI lines. Because the gateway appliances are non-proprietary equipment they can be simply and inexpensively expanded to support additional capacity and/or additional interface types as future needs arise.

The NGA 911 solution has been designed to adhere to the evolving NENA i3 standards. To ensure interoperability, NGA 911 participates in and contributes to the NENA Working Groups tasked with defining the i3 standards for ESInet, NGCS, and call handling. Towards that same end NGA 911 also participates in the NENA Interoperability Collaboration Events (ICE) held every 18 months. As a result, the research and development effort typically lead to a solution compliant with the NG9-1-1 standards in advance of the standards being formally approved and ratified.

NGA 911's Spatial Interface (SI) collects, verifies, and incorporates GIS 'attributes' and other datasets into the NGCS ECRF and LVF. During the transition to i3 from E9-1-1, NGA 911's SI also depends on an LDB (Location Database). NGA 911's LDB incorporates 'legacy' ALI/ANI, (pANI), MSAG, e2 steering, and other relevant routing data and attributes. The LDB can then be used to support legacy functions like the Location Interworking Function (LIF), ALI dips, vendor SOI updates, and act as a transitory LIS (Location Information Service) until such time as the State of Nebraska, neighboring States, and ingress OSPs are all operating off a unified i3 compliant GIS and location related FE's.

The primary motivation behind our network design philosophy is to utilize the best innovations in carrier grade technology to improve the reliability of emergency communications while driving down the cost. To achieve those dual goals, we are making heavy use of cloud hosting capabilities and SD-WAN on the ESInet. These two factors allow us to provide a solution that has an uptime reliability in excess of five 9s with a level of redundancy that would otherwise be uneconomic.

All of NGA 911's routing infrastructure, like the rest of the NGCS, is deployed in a robust, reliable, highly available, redundant manner as described throughout our response. Moreover, this robust routing infrastructure offers the full spectrum of diverse routing capabilities including jurisdictional, agency, incident, policy based, ad hoc, and dynamic. All routing equipment supporting the ESInet will be staged in a secure cabinet approved by the manufacturers.

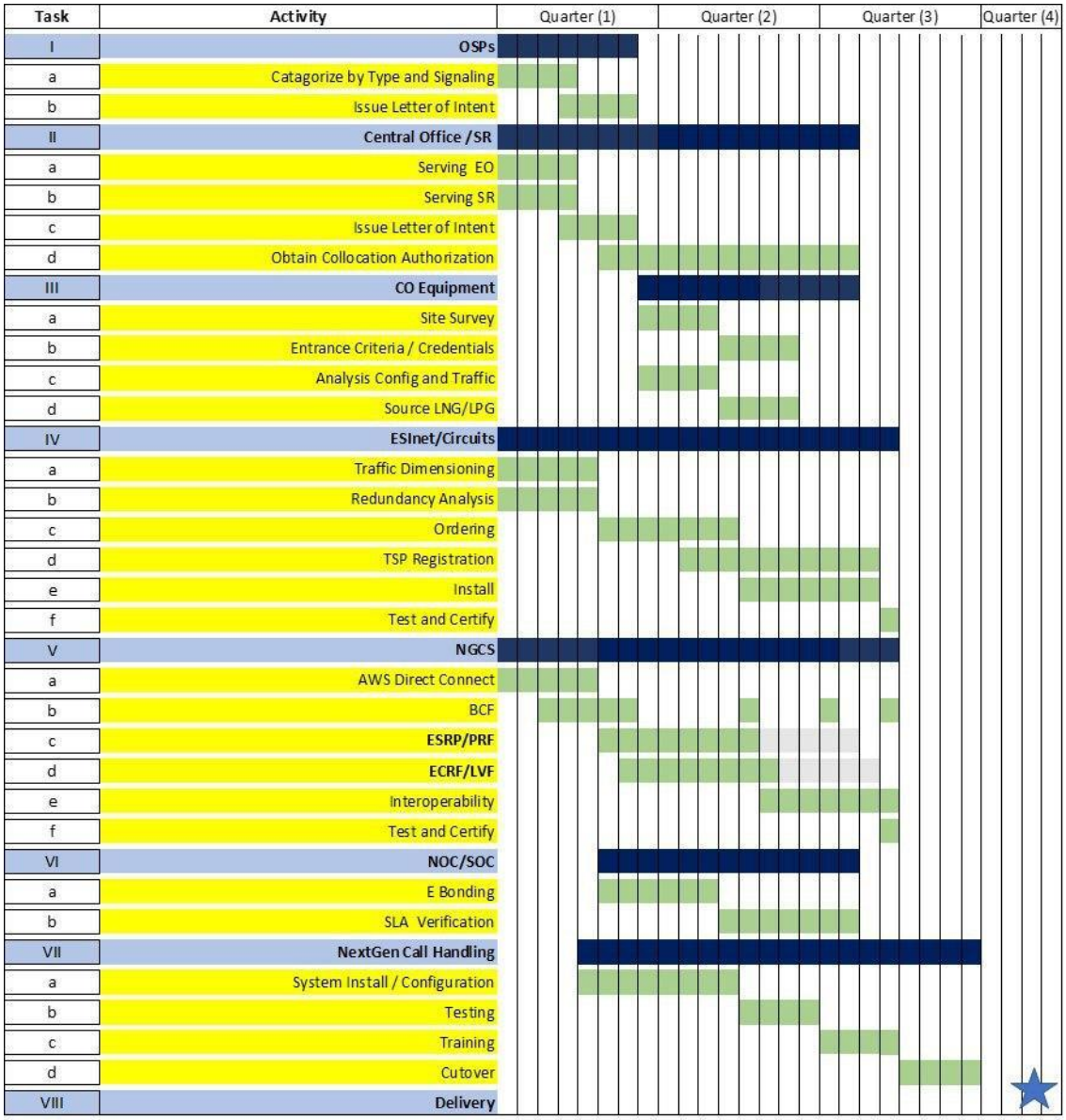
c) ATTACHMENT C – TECHNICAL REQUIREMENTS

Attachment C – Technical requirements has been included and labeled according to RFP requirements. NGA 911 has responded to Option A, Option B, and Option C.

d) PROPOSED HIGH-LEVEL PROJECT PLAN

The proposed high-level Project Plan has been included as a separate attachment and labeled according to RFP requirements.

e) SCHEDULE FOR THE LIFECYCLE OF THE PROJECT



f) COST PROPOSAL

The NGA 911 Cost Proposal has been provided as a separate attachment and labeled according to RFP requirements.

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

Bidders are instructed to complete a Matrix for Next Generation Core Services (NGCS). Bidders are required to describe in detail how bidder's proposed solution meets the conformance specification outlined within each Requirement. The matrix is used to document and evaluate bidder's response to the requirements.

The matrix should indicate how the bidder intends to comply with the requirement and the effort required to achieve that compliance. It is not sufficient for the bidder to simply state that it intends to meet the requirements of the RFP. PSC will consider any such response to the requirements in this RFP to be non-responsive and the bid may be rejected. The narrative should provide The Public Service Commission (PSC) with sufficient information to differentiate the bidder's business solution from other bidders' solutions. Bidder shall not refer to other sections as a response. Even if the response is an exact duplicate of a previous response, the details shall be provided in the same paragraph as the requirement. Bidder shall not include pricing information in the description and shall not refer the reader to pricing.

The bidder must ensure that the original requirement identifier and requirement description are maintained in the matrix as provided by PSC. Failure to maintain these elements may render the bid non-responsive and result in for rejection of the bidder.

The bidder's response to each of the below requirements shall include an indication on the level of compliance that can be met. (Complies, Complies Partially, Complies with Future Capability, Does Not Comply) Bidder shall respond by placing an "X" in only **one** checkbox per requirement. Failure to complete this process properly will be treated the same as "Does Not Comply," and may result in the rejection of the response form.

1. Complies: Bidder's proposal complies with the RFP requirements and the products/services are included in the base price, are currently developed, generally available, and successfully deployed. Responding with "Complies" or "Complies with Future Capability" shall mean the Bidder's solution meets or exceeds the requirement regardless of any comments included as additional information.

2. Complies Partially: Bidder's proposal addresses the RFP requirements through another method that currently is developed and available for implementation (i.e., shall be generally available), or the solution complies with some, but not all of the requirements. Bidder is responsible for clearly explaining how bidder's proposed solution does not fully comply.

3. Complies with Future Capability: The RFP requirements will be met with a capability delivered at a future date. This response shall include a calendar quarter and year in which the requirement will be met with a generally available product or service at no additional cost.

4. Does Not Comply: Bidder's proposal does not/cannot meet the specific RFP requirement.

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

Req. Identifier	Requirement Description				
GEN-1	**General Requirements - Bidder Vision of NG911** The Commission is issuing this RFP for the purpose of selecting a qualified bidder that understands and can clearly demonstrate alignment with the industry's evolution to NENA i3 -compliant ESInet and NGCS solutions. Describe bidder's vision of NG911 and how bidder's vision aligns with NENA's i3 standard, bidder's approach to monitoring and supporting evolving standards and the bidder's level of involvement in standards development and Industry Collaboration Events (ICE).	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			

Bidder Response:

NGA 911 personnel have been closely involved with the planning and development of NENA's i3 architecture since its inception in the early 2000s.

Monitoring and Supporting Evolving Standards and Best Practices

The NGA 911 ESInet and NGCS solution is NENA i3 compliant. NGA 911 will upgrade our systems to meet new standards within six months of issuance and approval. Before implementing an upgrade on the State's ESInet and NGCS, NGA 911 will work with the State to determine the benefits and drawbacks of the particular upgrades and if the State desires the features; NGA 911 will implement the upgrade under our comprehensive standards implementation process described below:

Beyond participation in the creation of NENA Standards, NGA 911 works with its customers, and the industry on the verification (Lab/Interoperability Testing), promulgation (Documenting), enforcement (Monitoring and Reporting), adjustment (Patching) and evolution (Updating) of our solution as new standards are approved. We accomplish all of the above systematically by use of a unique Agile DevOps process and Functional Element (FE) virtualization that allows us to run the original software elements side-by-side with updated software as a robust means to effectuate standards updates.

Industry Involvement

NGA 911 is fully committed to understanding industry trends and best practices and having a voice in shaping the industry for the greater good.

To stay current with the industry, NGA 911 actively participates in NG9-1-1 industry bodies such as NENA workgroups, the NENA Development Steering Committee (DSC), and iCERT, to name a few. Examples of successful participation include NENA ICE 7, preparation for participation in ICE 9, and successful testing with the Texas A&M Internet2 Technology Evaluation Center (ITEC) under the leadership of Dr. Walt Magnusson, Associate Director.

Our Standards Compliance Officer, Steve O'Conor, ENP, has served in the 9-1-1 industry for over 45 years. Since entering the private sector in 2011, Steve has been providing Next Generation 9-1-1 consulting services to public and private organizations

	developing and provisioning i3-conformant NG9-1-1 networks and services. Steve currently serves as Co-Chair of NENA's i3 Architecture Working Group, a position he has held for the past eight years, Co-Chairs the 9-1-1 Core Services Committee, and serves on the NENA Cloud Services workgroup. Previously, Steve served as NENA's President, served as Chair of NENA's Operations Committees, and co-chaired the Interconnection and Security Committee, which produced the industry-standard Next Generation 9-1-1 Security Standard (NG-SEC). Our CTO, Edmond 'Ed' Vea has served in the telecommunications and radio public safety industry since 1999, when as CEO of DETECON, his team provided the technical standards to the White House (now DHS) National Communications System - Wireless Priority Services for GSM. Later as the General Manager of an FGGE, Ed consulted with over 30 state and local government clients on Public Safety Land Mobile Radio, Broadband, and 9-1-1 systems. Ed has also served as a SME to the Department of Justice's OJP National Law Enforcement and Corrections Technology Center - Communications Center of Excellence and on the FirstNet Opt-Out projects in over 20 states. Our Senior Program Manager Shelly Guenther, ENP, has served the industry for 26 years. Shelly's background includes work as an Emergency Medical Technician (EMT), a 9-1-1 Dispatcher, and roles as a 9-1-1 Wireless Project Manager, Director of Voice over IP (VoIP), and NG9-1-1 Product Manager. Shelly currently serves as the NENA Development Steering Committee Co-Chair of the Data Management Committees. Darold Whitmer, SVP, Strategic Relationships, has over 27 years in 9-1-1 and over 15 years in NG9-1-1. Darold was a charter member of the NENA Next Generation 9-1-1 Partners Program (NGPP) in 2006 and worked with the USDoT on the NG9-1-1 trial program in 2010. The team at NGA 911, along with our deep commitment in the industry, provides an agile foundation allowing us to build, adapt, and implement new standards as they are approved. Our participation in these committees enables us to: 1) Help shape industry standards 2) Have foresight into the direction of NG9-1-1 3) Test the new standard/interface in our lab 4) Confirm the compatibility with carriers, our systems, and vendors 5) Collect invaluable, experiential information

	6) Document the process 7) Create an achievable plan for roll out The NGA 911 solution adheres to the following: · NENA-STA-010.2-2016 (formerly NENA 08-003), Detailed Functional and Interface Specification for the NENA i3 Solution · NENA 08-002, NENA Functional and Interface Standards for Next Generation 9-1-1 Version 1.0 (i3) · NENA 08-751, NENA i3 Technical Requirements Document · NENA 04-001, Recommended Generic Standards for E9-1-1 PSAP Equipment · NENA 75-001, Security for Next Generation 9-1-1 Standard (NG-SEC) · NENA – INF 15.1-2016, NENA NG9-1-1 Security Information Document · NENA 04-503, Network/System Access Security · NENA 75-502, Next Generation Security Audit Checklist · NENA – INF-016.2-2018 (formerly 08-506), Emergency Services IP Network Design for NG9-1-1 · NENA 08-752, Location Information to Support IP-Based Emergency Services Requirements · NENA 71-502, An Overview of Policy Rules for Call Routing and Handling in NG9-1-1 · NENA-STA-003, NENA Standard for NG9-1-1 Policy Routing Rules · NENA 08-506 Emergency Services IP Network Design for NG9-1-1 · Applicable Internet Engineering Task Force Standards (IETF), such as IP protocols, IP routing protocols, SIP, RTP, LoST, and PIDF-LO.

	Additional Standards and guidelines NGA 911 adhere to: · NENA-REQ-002.1-2016, NENA Next Generation 9-1-1 Data Management Requirements · NENA-STA-005.1.1- 2017, NENA Standards for the Provisioning and Maintenance of GIS data to ECRF and LVFs · NENA-STA-006.1-2018, NENA Standard for NG9-1-1 GIS Data Model · NENA-INF-011.1-2014, NENA NG9-1-1 Policy Routing Rules Operations Guide · NENA-STA-012.2-2017 (originally 71-001), NG9-1-1 Additional Data Standard · NENA-INF-015.1-2016, NENA NG9-1-1 Security Information Document · NENA STA-015.10-2018 (Originally 02-010), NENA Standard Data Formats for E9-1-1 Data Exchange & GIS Mapping · NENA-INF-023.1-2017, NENA Call Blocking Information Document · NENA-INF-024.2-2018 (originally 04-502), E9-1-1 PSAP Site Characteristics Technical Information Document · NENA-INF-027.1-2018, NENA Information Document for Location Validation Function Consistency · NENA-STA-028.2- 2018 (originally 04- 004), Generic Standards for E9-1-1 PSAP Intelligent Workstation (IWS) Equipment · NENA-INF-029.2-2018 (originally 04-501), Integrating Applications on Intelligent Workstations Technical Information Document · APCO/NENA 2.105.1- 2017, NG9-1-1 Emergency Incident Data Document (EIDD) (ANSI accredited) · NENA 08-501, Interface between the E9-1-1 Service Provider Network and the Internet Protocol (IP) PSAP Information Document · NENA 08-502, E9-1-1 Requirements Information Document · NENA 08-505, Methods for Location Determination to Support IP-Based Emergency Services Information Document The NGA 911 team has more than 375 years of 9-1-1 experience and over 100 years of NG9-1-1 experience.

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN-2	**Proprietary Solutions and Standards** 1. Describe any use of proprietary standards, interfaces, or protocols in bidder's proposed solution. 2. Describe any patented technology in the proposed solution, who owns the patent and describe any licensing arrangements. Disclose any technological limitations, in the response. .	X			
	Bidder Response: NGA 911 does not have any proprietary standards, interfaces, or protocols in the NGA 911 proposed solution. NGA 911 holds Patent # US 10,542,146,B2, NEXT GENERATION EMERGENCY CALL ROUTING OVER DIVERSE NETWORKS. As NGA 911 owns this patent there are no licensing fees. NGA 911 does not have any undisclosed technological limitations.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN-3	**System and Network Architecture** The Commission is seeking a Public Safety Grade Next Generation 911 System. System and network architecture, including the design and deployment of interface functions and security measures, shall comply with current NENA i3 requirements as established in NENA-STA-010.2-2016, NENA Detailed Functional and Interface Standards for the NENA i3 Solution. Describe how the solution meets or exceeds the above requirements	X			

Bidder Response:

Public Safety Grade

NGA 911 designs, engineers and deploys the ESInet and the NGCS to exceed Public Safety Grade as defined in Section V.D.1.b. of the RFP. As noted in the Section, the term "public safety-grade" has been utilized to refer to this level of standards compliance; however, a universal definition of this term has not been proposed by a Standards Development Organization (SDO). The public safety industry accepted standard for public safety grade systems and networks is five nines (99.999%). NGA 911 exceeds 99.999% reliability and availability as a matter of course. NGA 911 never relies on a single network service provider for ESInet connectivity. We aggregate and bond broadband trunk circuits from at least 3 providers. For the NGCS, we utilize a diverse cloud based virtual infrastructure that is geographically diverse and built upon 8 cores in two regions and four availability zones. Our NGCS can scale to cover the call volume of over 125% of the whole United States in minutes, always staying well ahead of 9-1-1call demand.

Reliability and Availability

With eight (8) cores and a fully meshed access network, NGA 911's NGCS architecture provides a multi-layered redundancy of systems, software, and facilities with no single point of failure. Our solution exceeds 99.999% availability with the hardened infrastructure of Amazon Web Services (AWS). AWS has proven re-routes, resiliency, redundancy, and reliability. NGA 911 replicates critical system components across multiple Availability Zones (AZs) to ensure high availability both under normal circumstances and during disasters such as fires, tornadoes, or floods. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities. Each AWS AZ runs on its own independent infrastructure, engineered to be highly reliable so that even extreme disasters or weather events should only affect a single AZ. The data centers' electrical power systems are designed to be fully redundant and maintainable without impact to operations. Common points of failure, such as generators, UPS units, and air conditioning, are not shared across AZs.

By deploying an instance of the NGCS in 8 availability zones in 8 cores, NGA 911 significantly exceeds 99.999% availability for the NGCS as calculated below:

Diagram GEN-3-1: NGA 911 NGCS Availability Calculations

NGCS	Non Redundant 1 AZ		Redundant 2 AZ		Redundant Region 2 AZ's each	
Functional Element	**Signaling**	**Media**	**Signaling**	**Media**	**Signaling**	**Media**
AWS Data Element	*99.999%*	*99.999%*	*>59's*	*>59's*	*100%*	*100%*
BCF	*99.99%*		*>59's*		*100%*	
ESRP	*99.95%*	*99.95%*	*>59's*	*>59's*	*100%*	*100%*
ECRF	*99.95%*		*>59's*		*100%*	
LVF	*99.95%*		*>59's*		*100%*	
	99.84%	**99.95%**	**>59's**	**>59's**	**100%**	**100%**

Diverse Data Connections – NGA 911's design provides for two separate network providers to serve the PSAP. Beyond the inherent diversity of two different network providers NGA 911 has a desire to provide diverse North/South conduits to connect to the NGCS.

Fault Tolerant Architecture for SIP with B2BUA **-** The NGA 911 fault tolerant architecture has been designed to handle SIP/RTP traffic across the NGCS to communicate to each AZ. Each SIP/RTP connection is separate and distinct. Both are recipients of the benefits of redundancy at the Region, Availability Zone, and Instance level of the architecture. Furthermore, both are supported by the fault tolerant RDBMS Cluster and File Services. And finally, B2BUA with proper anchoring ensures fluid failover paths for resilience.

Fault Tolerant Architecture for HTTPS **-** The fault tolerant architecture for handling HTTPS traffic across NGCS. Similar in design to the SIP/RTP architecture, HTTPS architecture is separate and distinct for SIP/RPT. HTTPS, like SIP/RTP is the recipient of the benefits of redundancy at the Region, AZ, and Instance level of the architecture. Furthermore, HTTPS is supported by the fault tolerant RDBMS Cluster and File Services.

Machine Images (MI) - MI is a web service within the Infrastructure-as-a-Service (IaaS) that provides computing resources –server instances – that we have used to build and host the NGCS. We have built a library of MIs, so replacing a failing instance is very simple; we just launch a replacement instance that uses the same MI as its template.

This is just the first step toward fault tolerance. The NGA 911 NGCS is able to quickly recover from failures; if an instance fails, or is not behaving properly, it is immediately and without human intervention taken offline and another instance based on the same

	template takes over. To exceed five nines (99.999%) uptime reliability, there are 8 instances of the NGCS running at anyone time each with the ability to process 100% of the Nebraska call volume. **Signaling and Media Delivery Network** NGA 911 exceeds the PSG requirement through our diverse engineering of the "last mile" by being carrier agnostic and seeking geographically and carrier diverse networks. . As a result, NGA 911 is able to leverage state and commercial assets. NGA 911's primary concern is the value of survivability, reliability, and connectivity of the network. NGA 911 never settles for the status quo and will constantly, through the term of the contract, look to leverage existing assets to provide better performance to the State of Nebraska. NGA 911 is providing a High Availability (H/A) SD-WAN interface solution to all Endpoints (PSAPs, Aggregation Points, and Direct Connect Facilities). The SD-WAN seamlessly bonds diverse IP based interconnections (WANs) into a single integrated connection. Note: The SD-WAN handles BGP (Layer 2 or Layer 3) at each PSAP and at additional points based on mutually agreed connections to the data centers. The SD-WAN is transport independent and is centrally managed by NGA 911. It offers a shared VPN schema across any WAN circuit (i.e. Microwave, LTE, MPLS, broadband, etc.) and supports flexible VPN extension to all endpoints (IaaS, PSAP branch, PSAP Data Centers) with a supporting SD-WAN appliance. The SD-WAN technology deployed end-to-end by NGA 911 appends flow tracing packets to each and every packet traversing the whole ESInet from ingress to egress whether signaling or media. These "sidecars" are used to measure latency, jitter, route, and travel times for each and every route and interconnect service provider on the net. This includes signaling (meta data); media information such as codec and protocol; network performance logs for latency, jitter, and packet loss; and Mean Opinion Score (MOS) and other quality indicators of fidelity. The logging begins from ingress as a call is received from an Originating Service Provider (OSP). Any transcoding is noted and validated. A MOS score is recorded at ingress to be used for comparison at egress. Additionally, the SD-WAN binds the diverse provider's connections into dual aggregate connections that permit a media comparator function. The real time and historical data gathered from the SD-WAN offer an unprecedented view of the overall and specific network service provider performance allowing SLA's to be managed and enforced. The NGA 911 NGCS requires Firewalls as part of the BCF/SBC functions. The SD-WAN includes a Zone-based, Stateful firewall. NGA 911's service also includes Zscaler for Deep Package Inspection (DPI) on the cloud. NGA 911 will also provide additional firewall solutions when needed as part of our defense in depth security package. **Security**

	NGA 911 secures communications by applying and adhering to the measures, as recommended in NENA-INF-015.1-2016, Section 3.2 and is fully compliant with NG-SEC. NGA 911 maintains a living security document known as the Security Policy Note (SPN) which is the basis of our defense to protect all layers of the IP protocol stack. The SPN takes into account and complies with the NENA NG-SEC 75-001 Audit Checklist. Additionally, NGA 911 leverages the vast body of activities and knowledge dedicated and committed to Cybersecurity to ensure a constant refresh of cybersecurity policies. The National Institute of Standards (NIST) is a primary go-to organization for this information and a leader in combating cyberthreats. On April 25, 2019, NIST released the "NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1" which covers new areas including Cyber-Attack Lifecycle, Internet of Things, Measuring Cybersecurity,w Referencing Techniques, and Secure Software Development. **National Standards and Public Safety Grade** NGA 911 confirms that our service and components exceed the national standards listed in Table1 of Section V.D. and the public safety grade definition in Section V.D.1.b.

Any additional documentation can be inserted here:

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

<table>
<tr><td rowspan="3">GEN-4</td><td rowspan="2">General Requirements – Capacity- Initial Design and Deployment
The bidder's initial design and deployment of the ESInet and NGCS elements, including all components and physical network segments, shall provide capacity that will support current and planned ESInet traffic and usage that occurs as a result of data sharing in, and between, all participating PSAPs, the Commission, and designated support agencies. Additionally, the system and network design shall allow for 50 percent traffic and usage growth for the life of the contract. All current and potential core functions and applications shall be considered, e.g., call-handling systems, CAD, logging, GIS data, streaming media, real-time text (RTT), IP traffic, traffic management systems, communications systems, and incident management systems. Describe how bidder's solution will meet or exceed the above requirements.</td><td>Comply</td><td>Partially Comply</td><td>Complies with Future Capability</td><td>Does Not Comply</td></tr>
<tr><td>X</td><td></td><td></td><td></td></tr>
<tr><td colspan="5">Bidder Response:
The NGA 911 initial design and deployment of the ESInet and NGCS elements will provide the capacity to support current and planned ESInet traffic and usage. Different types of traffic offer varying loads to the networks and should be segmented and handled via DiffServ Code Point (DSCP) in accordance with industry standards. DSCP is defined in NENA i3 as a means of classifying and managing network traffic using the 6-bit Differentiated Services (DS) field in the IP header for packet classification.

Working together with the State, we will start with the following Per Hop Behaviors (PHB) on the BCF ESInets BCFs, which we will adjust based on operational experience.

We will specifically address the current and potential core functions and applications including, call-handling systems, CAD, logging, GIS data, streaming media, real-time text (RTT), IP traffic, traffic management systems, communications systems, and incident management systems.</td></tr>
</table>

DSCP	Use		PHB
1	Routine Traffic	IP Traffic Logging Administrative Access	Defa ult
5	9-1-1 Signaling	SIP ADR and EIDO for Call Handling System (data) CAD (data)	AF12
9	9-1-1 Text Media	RTP/Streaming Media	AF12
13	9-1-1 Audio Media	RTP/Streaming Media	EF
17	9-1-1 Video Media	RTP/Streaming Media	AF11
21	9-1-1 Non-human-initiated Call	Alarms Telematics Internet of Things etc	AF21
25	Intra ESInet Events	Policy Routing Rules API Traffic Management Systems GIS data Incident Management Systems	AF21
29	Intra ESInet Other 9-1-1 Traffic	Non Critical	AF22

The NGA 911 BCF and Network Orchestration system has finer controls to manage all aspects of the Network. We start with an emphasis on REAL TIME MEDIA as the fundamental service of an NGCS based ESInet. From this foundation we consider the following tools when applying a traffic shaping strategy for the state:

Aggregate = Our NG Trunk Service rakes up common Layer 2 and Layer 3 links from MPLS, MEF, ELAN, LTE, 5G, MW etc.

Bond = Aggregated links may be 'bonded' together presenting a unified L2 or L3 Service.

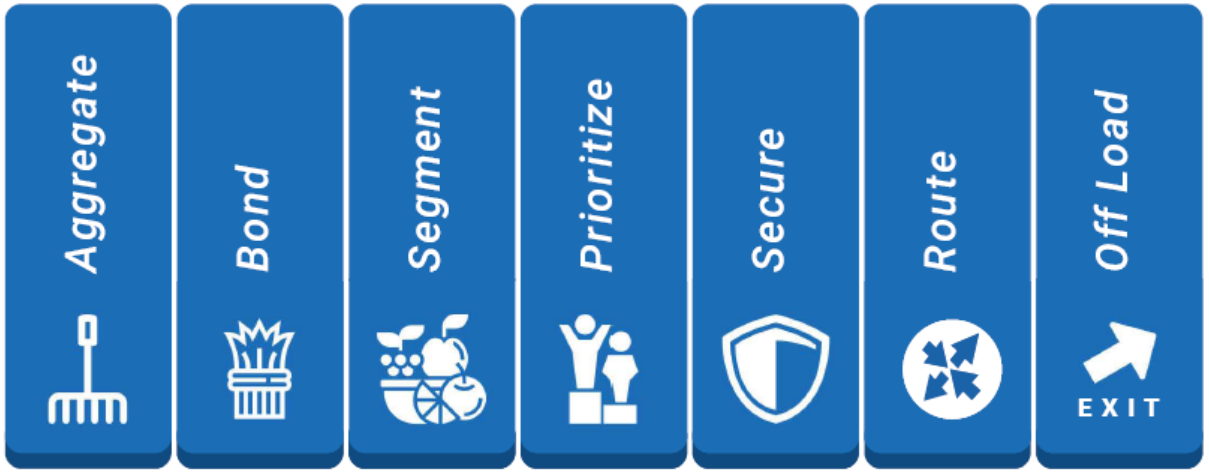
Segment = Although aggregated and bonded, application level services running over our NG Trunks can be segmented into any number of categories (e.g. voice, text, video, data, HD, best effort, etc.).

Prioritize = Segmentation without differentiation is no better than 'best=effort', so on top of it; prioritization and bandwidth reservation are applied.

Secure = In addition to all the traditional methods a defense in depth security posture brings, security is enhanced by the layering inherent in aggregation, bonding, and segmenting of traffic.

Route = Segmented and Prioritized services and media are ready for Slicing and Routing at Scale.

Off Load = The heart of Next Gen Communications is the ability to service applications at the most efficient point: the core, the edge, or locally. Our "off load' feature uses AI and ML to dynamically and uniquely determine where that point should be for each function and service.



ESInet

The NGA 911 deployed ESInet takes into account all of the different traffic types, volumes, and priorities in properly dimensioning the network. In this case there are two layers to the ESInet the Inter-Region network that aggregates the OSP traffic for the state for distribution to the Regional and Independent PSAPS). A regional PSAP will generally have a hosted CPE. The network of the hosted CPE may or may not be part of the ESInet, but in Nebraska, for now, the connectivity from the Host sites to the PSAPs is outside the scope of the response and is therefore not included.

NGCS

The NGCS is made up of virtual infrastructure supporting the functional elements that correspond to the NENA i3 model and include: BCF, ESRP, PRF, ECRF, LVF, LDB/LIS, SI and transitional components such as the LNG (PIF, LIF, NIF), LSRG, and LPG functions.

NGA 911 considered the following when conducting our initial capacity calculations:

NG9-1-1 End to End Traffic

- Covered population
- OSP type and offered traffic distributions
- Traffic type and distributions

Ingress Traffic

- OSP Type
- Traffic Volumes and Distributions

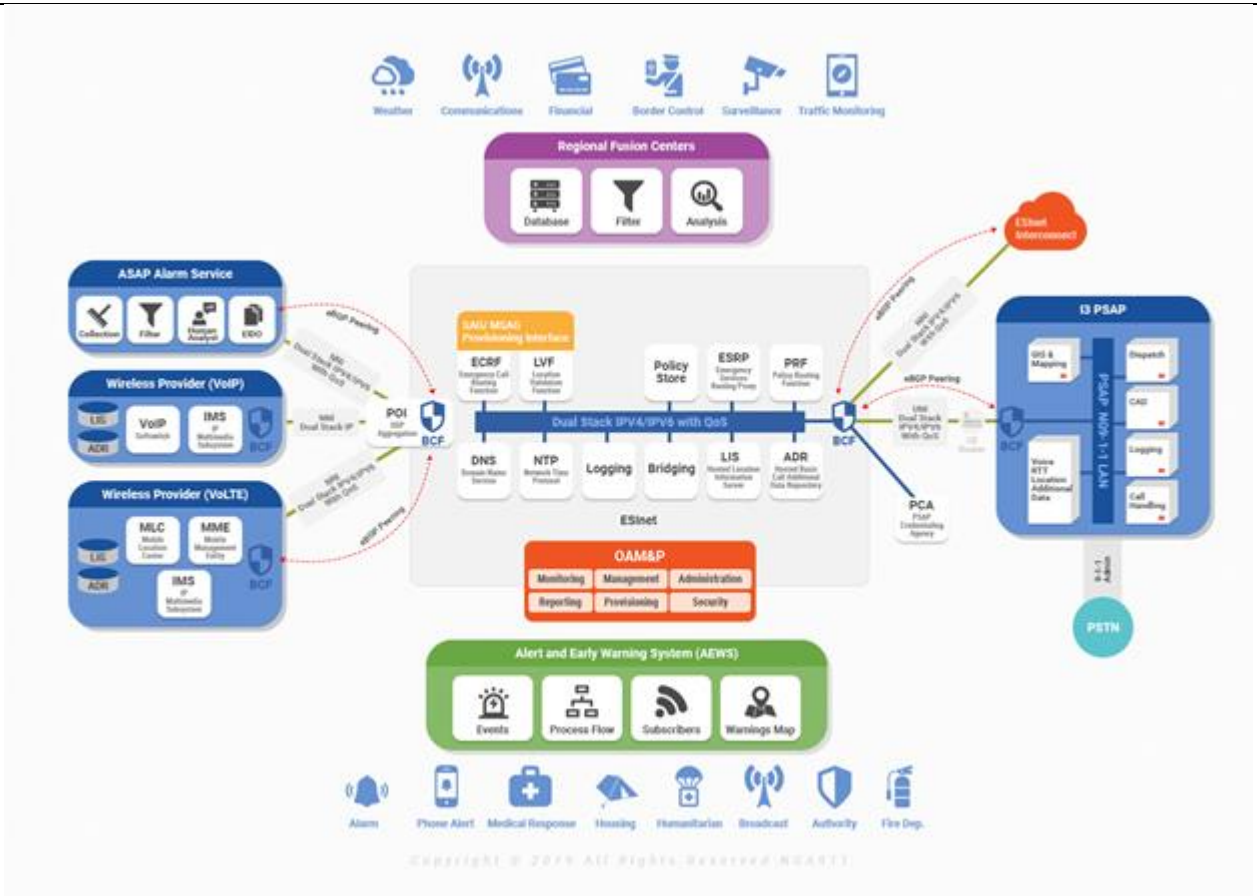
Apps and Services

- CAD
- Logging
- Traffic Management
- Incident Management Systems
- Support Agencies MIS

	Interoperability • Call Transfers • Data Sharing • Load Sharing • ESInet to ESInet

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN-5	**Scalable Deployment** As the Commission migrates toward a fully compliant NG911 environment, additional PSAP functions will transition to the systems and network. The bidder's systems and network solution shall be designed and deployed in a way that is easily scalable, with the capability to grow in both capacity and coverage without disruption in service. Describe in detail how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The NGA 911 NG9-1-1 Environment is built upon a flexible virtual cloud based infrastructure designed specifically to to be fully NENA i3 compliant Functions elements are instantiated on supporting infrastructure based on CPU, Storage, and I/O demands which are directly related to processing requirements, data generation and use, discrete communications between elements and functional dependencies. The distribution of FE's across self-healing instances provides for a solution that scales to meet demand and to heal from component failures. **Future PSAP Functions.** The future of PSAP function is seemingly unlimited from the now available Real Time Text (RTT) and added services from Incident and Location Routing, Government Fusion Centers, Alarms and Surveillance, Telematics/Internet of Things, and Early Warning Systems/PSAP to Citizens to name a few.				



Incident and Location Based Routing

The benefit of NG9-1-1 when implemented by NGA 911 is comprehensive integrated location based routing. The next step is to leverage that power of location to manage incidents better by directing traffic on the network based on location, incident, and service

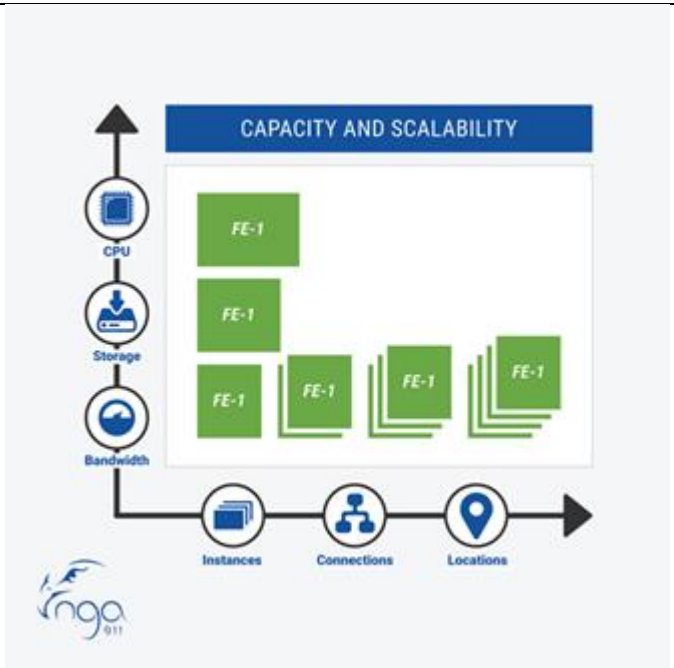
	requests (URNs). The NGA 911 NGCS is already architected to take full advantage of our relationships with commercial and government systems and providers capable of providing accurate and verifiable location data on day one. **Government Fusion Centers** In the near future government fusion centers at the regional, state, and Federal level will be able to provide inputs that will enable PSAPs to organize and direct incoming service requests in a more robust manner. **Telematics/Internet of Things** Similar to Alarm and Surveillance service requests, as automobiles, buildings, and machines are equipped with sensors and broadband (4G/5G) connections, there may be PSAPs and 9-1-1 authorities that will want to leverage it. The NGA 911 Incident Management Infrastructure is ready to incorporate it from a process and technical point of view. **Early Warning Systems/PSAP to Citizen** The NG9-1-1 Alert and Early Warning System (AEWS) is already compliant with IPAWS latest directive for permissions, proficiency, user-interface, confirmation, and error checking. The AEWS directs authenticated CAP v1.2 compliant notifications to FEMA's IPAWS Open Platform for Emergency Networks (IPAWS-OPEN). All notifications are validated and authenticated prior to secure transmission to OPEN. Authentication on AEWS utilizes the Identity, Credentialing, Access Management (ICAM) processes using a hierarchical structure for credential management. The ICAM system will be aligned with the Statewide Emergency Management System if available. ICAM includes providing for the necessary Web Service Certificates, digital signatures, ensures non-repudiation and message integrity as required by FEMA and IPAWS. NGA 911's AEWS enables PSAPs to proactively provide Amber Alerts, Weather Updates, and other Public Information directly to citizens based on their location and or subscription information.

Interactive Voice Response (IVR)

IVR is not typically used in today's PSAP environment due to legislation, regulation or policy; however, it is available in the NGA 911 solution. When 100's of calls are located within the scene of an incident, it is possible that the caller is just a reporter and not a victim. An IVR can query whether the caller is just reporting the incident by providing a short description of the incident and asking the caller to affirm whether that is the reason for their call. Even if they answer in the affirmative, the IVR will ask if they still desire to speak to a person.

Scalable, Agile Design.

By design and intent, the NGA 911 ESInet and NGCS is deployed to be easily scalable, with the capability to grow in both capacity and coverage without disruption in service.



NGA 911 has already proven its ability to process large call volumes at a moment's notice for a population of 500,000,000 (150% of the U.S. population) with 300,000,000 9-1-1 calls per year (125% of the U.S. total call volume). Tests were conducted per Internet Engineering Task Force (IETF) RFC 7502 Methodology for Benchmarking Session Initiation Protocol (SIP) Devices: Basic Session Setup and Registration (see Diagram GEN 5.2). As a system fundamentally designed with auto-scaling the concept of a single instance/container does not exist for our architecture. Even if traffic was somehow restricted to one Availability Zone (AZ), the system upon reaching certain thresholds spins up additional containers with additional CPU, bandwidth, speed, and storage to stay well ahead of the demand.

Table of Internet **Engineering Task Force (IETF) RFC 7502 Methodology for Benchmarking Session Initiation Protocol (SIP) Devices: Basic Session Setup and Registration Test Results.** The tests had the following load:

Simulated Load

	Population: 500,000,000 Call per Year: 300,000,000 Number of PSAPs: 4,400 Call Takers: 18,000 Average Call Duration: 120 Minimum Call Duration: 10 Maximum Call Duration: 600 Under heavy load the system demonstrated vertical scaling, process distribution, and horizontal scaling with zero error.

Any additional documentation can be inserted here:

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SEC 1	**Security - Cybersecurity** For the purposes of this RFP, cybersecurity (security) is considered to be the established systems and processes focused on protecting computers, networks, programs, and data from unintended or unauthorized access, modification, or destruction. **Security Requirements and Standards** The security requirements established in applicable standards listed in Section V.D.1. Table 1 of the RFP apply equally to all elements of the system requested in this RFP, including but not limited to components located in the following building types: 1. Data centers; 2. Network-housing structures; and, 3. Regeneration sites and other buildings housing any element or device that is part of the overall system. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: NGA 911's proposed system adheres to all of the 16 security requirements listed in V.S.1 Table 1 for our: 1) Data centers 2) Network-housing structures 3) Regeneration sites and other buildings housing any element or device that is a part of the overall system NGA 911 is a standards-based solution that complies with nationally accepted standards and requirements applicable to ESInet architecture, security, and interface functionality. NGA 911's proposed system design, deployment, operation, and security will be in full compliance with the standards, requirements, and recommendations located in Table 1: Adopted Standards. Standards Development Organizations (SDOs) include: **i.** **Association of Public Safety Communications Officials (APCO)** **ii.** **The Monitoring Association (TMA)** **iii.** **National Emergency Number Association (NENA)** **iv.** **Alliance for Telecommunications Industry Solutions (ATIS)**				

v. **Department of Justice (DOJ)**

vi. **Internet Engineering Task Force (IETF)**

vii. **North American Electric Reliability Corporation (NERC)**

viii. **National Institute of Standards and Technology (NIST)**

ix. **Telecommunications Industry Association (TIA)**

NGA 911 complies with the requirements by following our Process Adherence Policy maintained by Operations and our comprehensive Security Policy Note - Security Framework and Requirements v_f_2020 maintained by our Security Management Division. These Policies are readily available to our team and combined with the Process Sheet are used to track State and Federal Laws, Policies, Standards, and Codes. Our Processes are kept up to date. Our team is assigned tasks for accountability. To ensure compliance we have: Ongoing processes, Risk Assessment, Regular review and Gap Analysis, Monthly Training, Full documentation, and External Auditors.

NGA 911 strictly adheres to the limiting of access to our network and NGCS equipment to credentialed authorized personnel.

1) Process to request and receive log information

- The PSAP appointed Single Point of Contact (SPoC) will provide the NGA 911 Project Manager the following information for each person to have credentials:
  - Name, Date of Birth, Email Address, Role, and Jurisdiction they are allowed to have access to.
- The NGA 911 Service Team will build the profile.
- The NGA 911 Service Team will provide the login information to the end user.
- The NGA 911 Team will provide Admin, Train the Trainer, and End User training.
- The PSAP SPoC will update the NGA 911 Service Team of updates, changes, or deletes for authorized credentialed users.

2) Detailed explanation of its access control processes and procedures for logging physical access to IP network components, and how it generates the required reports monthly. NGA 911 will furnish monthly reports on Physical access to the NGA 911 ESInet and NGCS facilities, including failed attempts. Physical access to all data centers housing IT infrastructure components is restricted to authorized data center employees, vendors, and contractors who require access in order to execute their jobs. Access to facilities is only permitted at controlled access points requiring multi-factor authentication designed to prevent tailgating and ensure that only authorized individuals entering our data center. On a quarterly basis, access lists and authorization credentials of personnel with

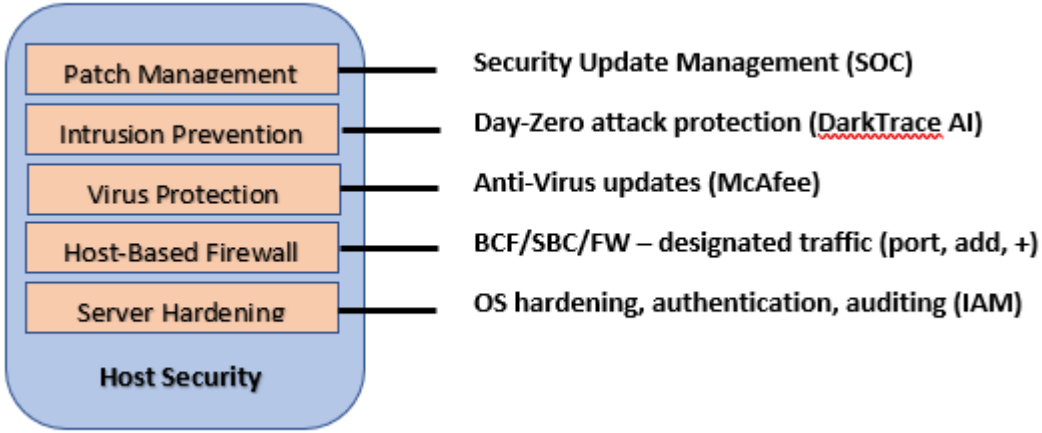
	access to data centers housing systems and devices within the system boundary are reviewed by the respective data center Area Access Managers (AAM). • All entrances to data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms if the door is forced open or held open. • Trained security guards are stationed at the building entrance 24x7x365. • If a door or cage within a data center has a malfunctioning card reader or PIN pad and cannot be secured electronically, a security guard is posted at the door until it can be repaired. • In order to provide physical security at the PSAP, NGA 911 recommends a locked cabinet in a secure telecommunications room.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SEC 2	**Security - Cybersecurity** **Security Plan** A comprehensive security plan is a critical component of the Nebraska's NG911 network solution. Describe the security plan, including the mitigation, monitoring, alerting, and incident-response processes; and, provide information on specific hardware components and software systems incorporated in the proposed security plan. The proposed solution's security plan is required to utilize the latest NENA specifications and incorporate the intentions of the Communications Security, Reliability and Interoperability Council (CSRIC) and Task Force on Optimal PSAP Architecture (TFOPA) best practices.	X			

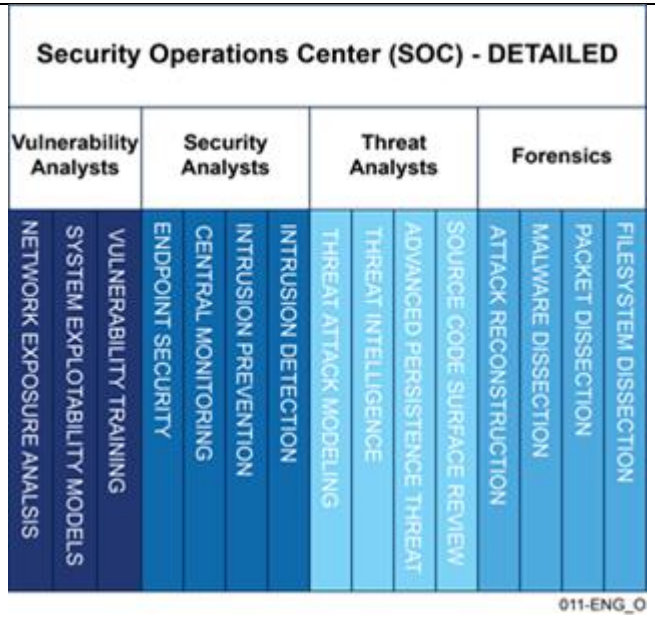
Bidder Response:
The NGA 911 solution's security plan utilizes the latest NENA specifications and incorporates the intentions of the CSRIC and TFOPA best practices.

Below is the security architecture diagram:



Host Layer

	A key component of our Host Layer Defense in Depth Security posture has a number of features and functions for avoiding, minimizing, and limiting malicious activity that may occur at any point within the NGA 911 ESInet and NGCS system. The focus of malicious activity is on Core Security which is built upon the following elements. • Server Hardening • Host Based Firewall • Virus Protection • Intrusion Prevention • Patch Management Server hardening involves making sure our OS is hardened, which in large part, is handled through the use of Docker Containers. Access to the containers is strictly managed through our IAM. Host based firewalls are covered by the comprehensive application of the inherent BCF/SBC/FW functions and elements we built into the network in accordance with the specifications. Virus protection is covered by subscriptions (managed by the SOC) to several leading Anti-Virus software providers. Intrusion prevention in addition to intrusion protection detailed below is managed through Artificial Intelligence - AI (the details are subject to confidentiality protections and a need to know basis) that quickly identifies, monitors, and reports anomalies that might be the result of a day-zero attack. And finally, this is all managed by our SOC processes and procedures as detailed and maintained in our SPN. **Security Operations Center (SOC)** The heart of Cybersecurity monitoring and response is our SOC which is subdivided into four major areas of focus: vulnerability and security assessments and analysis, threat research, and forensic capabilities. Each of these is broken down to sub focus groups for a comprehensive approach to surveillance, identification, mitigation, and recovery. The details of the NGA 911 Security Process Flows are detailed in our confidential Security Policy Note, which can be provided to the State's Security Auditor during a formal audit of our security policies and procedures.



In addition to the above-mentioned process flow, the Security Operations Center (SOC) provides alerts and notifications of suspicious events such as: malware activity, ransomware activity, and port and protocol exploitation. When issues arise, the SOC provides the ISP, ICC and PSAPs:

- Alert and notification of activity noticed to the Board/designated staff and the affected PSAPs
- Details on the options for isolation of activity to limit impacts and vulnerabilities
- And notifies the ISP, ICC and PSAPs of any limitations that may result through executing the avoidance measures

Any additional documentation can be inserted here:

SEC 3	**Security - Cybersecurity** **Security Compliance Matrix** Describe how the proposed solution addresses compliance in each of the following categories in NENA 75-502, NENA NG-SEC Audit Checklist.

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

Category
1. Senior Management Statement
2. Acceptable Use Policy
3. Authentication/Password Policy
4. Data Protection
5. Exception Request/Risk Assessment
6. Hiring Practices
7. Incident Response
8. Information Classification and Protection
9. Physical Security
10. Compliance Audits & Reviews
11. Network/Firewall/Remote Access
12. Security Enhancement Technical Upgrade
13. Technical Solutions Standards
14. Wireless Security

Bidder Detailed Response:
NGA 911 complies with all sections and aspects of the Security Audit Checklist. NGA 911 has attached a Security Audit Checklist and labeled according to RFP requirements.

Any additional documentation can be inserted here:

	Security - Cybersecurity **Predictive Analysis and Monitoring** Describe solution's capabilities to provide predictive analysis and modeling to combat security threats.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
SEC 4	Bidder Response: As part of our Defense in Depth Approach, NGA 911 adheres to predictive analysis and modeling to combat security threats. The NGA 911 network runs an Intrusion Prevention System (IPS) capability within the Border Control Function (BCF) network firewall to monitor and evaluate network traffic to detect and prevent network threats from entering the NGCS. The IPS is integrated with the network gateway to provide the ability to apply IPS signatures to Internet Protocol (IP) packets within the GPRS Tunneling Protocol (GTP) User (GTP-U) plane tunnels and GTP Control plane (GTP-C) tunnels. The IPS will intercept packets and inspect traffic for various threats (such as signaling storms). This allows for an automatic pass/drop packet decision, plus enables the Security Operation Center (SOC) to monitor and log any malicious events. The IPS also uses unique traffic-learning algorithms to effectively detect network anomalies and block traffic outside of configured thresholds. This effectively stops Distributed Denial of Service (DDoS) attacks and other threats characterized by unusual traffic patterns. There is also built-in signaling support for Session Initiation Protocol (SIP) to protect voice, text, and media infrastructure and RTP traffic. NGA 911 uses state of the art Cyber Intrusion technology to track possible attacks and unauthorized access while implementing IPSec (3GP TS 33.210) protocols to protect 9-1-1 traffic between the NGCS and the PSAP sites. IPSec will utilize IKE V2 and PKI for peer authentication. BCFs will be used between the state infrastructure and outside networks to secure data on potentially untrusted networks for network domain security. Inter Core element signaling will be protected across the transport networking utilizing Group Domain of Interpretation (GDOI) VPNs and site-to-site VPNs, as appropriate. Advanced Encryption Standard (AES) 128/256 encryption will be available over interconnection networks on both fiber and microwave links to ensure all traffic is secure from outside monitoring. Firewalls will be used to protect all interfaces to ESInet against TCP sweeps, denial of service attacks (i.e., bandwidth saturation attacks), botnet attacks, and IPv6-related DDOS attacks, among other of the ever-increasing threats against mobile networks. A key component of our Host Layer Defense in Depth Security posture has several features and functions for avoiding, minimizing, and limiting malicious activity that may occur at any point within the NGA 911 ESInet and NGCS system. The focus of malicious activity is on Core Security which is built upon the following elements. • Server Hardening • ESInet Based Firewall • Virus Protection • Intrusion Prevention • Patch Management				

	Server hardening involves making sure our OS is hardened which in large part is handled through the use of customer Docker Containers. Access to the containers is strictly managed through our IAM. ESInet based firewalls are covered by the comprehensive application of the inherent BCF/SBC/FW functions and elements we built into the ESInet in accordance with the specifications. Virus protection is covered by subscriptions (managed by the SOC) to several leading Anti-Virus software providers. Intrusion prevention in addition to intrusion protection detailed below is managed through Artificial Intelligence - AI (the details are subject to confidentiality protections and a need to know basis) that quickly identifies, monitors, and reports anomalies that might be the result of a day-zero attack. And finally, this is all managed by our SOC processes and procedures as detailed and maintained in our SPN.

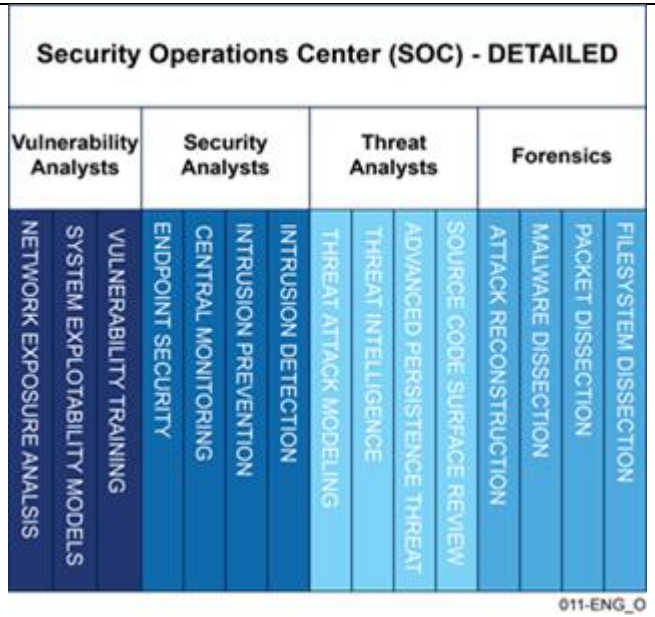
Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SEC 5	**Security - Cybersecurity** **Credentialing Process** Solution shall provide a process so that devices and carriers outside the IP network shall not have credentials, per NENA-STA-010.2-2016. Provide details regarding how the solution ensures that devices and carriers outside the IP network are not provided credentials.	X			
	Bidder Response: The NGA 911 proposed solution adheres to the NENA-STA-010.2-2016 (formerly NENA 08-003), Detailed Functional and Interface Specification for the NENA i3 Solution. NGA 911 adheres to the Network Traffic Restrictions such that all data traversing the IP network, and subsequent access to that data, is restricted to public safety use only, as required in NENA-STA-010.2-2016,6 Section 3.7. Commercial and non-public safety data and access are strictly prohibited from sharing bandwidth dedicated for the NGA 911 ESInet use. Our Identity, Credentialing and Access Management (ICAM) system provides access only to properly credentialed and certified agents. Prior to the establishment of the PSAP Credentialing Agency (PCA), NGA 911 and the State IT department will agree on an interim agent credentialing method. We recommend that access be permitted only through multi-factor authentication and all attempts, whether successful or not, are logged and analyzed for anomalies. The NGA 911 ICAM Manager will grant devices and agents credentials to ensure that devices and carriers outside our IP network are not provided credentials.				

Any additional documentation can be inserted here:

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SEC 6	**Security - Cybersecurity** **Third-Party Security Audits** Bidder shall allow for annual third-party security audits at the request and cost of the Commission. Describe bidder's current process for third party security audits.				
	Bidder Response: NGA 911 will allow annual third-party security audits at the request and cost of the Commission with reasonable notice of 30 calendar days or as agreed to with the Commission. The audit will include but not limited to: 1. Whitelisted scanning and manual testing of the application only, with application credentials equal to the least privileged role within the application. 2. Manual verification of scan results with the same credentials. 3. Manual testing of the application for vulnerabilities. 4. Internal audits and system scans for vulnerabilities quarterly for the first year following deployment of the first PSAP and annually for the remainder of the contract and report findings to the State with recommendations for improvements.	X			



In addition to the above-mentioned process flow, the Security Operations Center (SOC) provides alerts and notifications of suspicious events such as: malware activity, ransomware activity, and port and protocol exploitation. When issues arise, the SOC provides the ISP, ICC and PSAPs:

- Alert and notification of activity noticed to the Board/designated staff and the affected PSAPs
- Details on the options for isolation of activity to limit impacts and vulnerabilities
- And notifies the ISP, ICC and PSAPs of any limitations that may result through executing the avoidance measures

Any additional documentation can be inserted here:

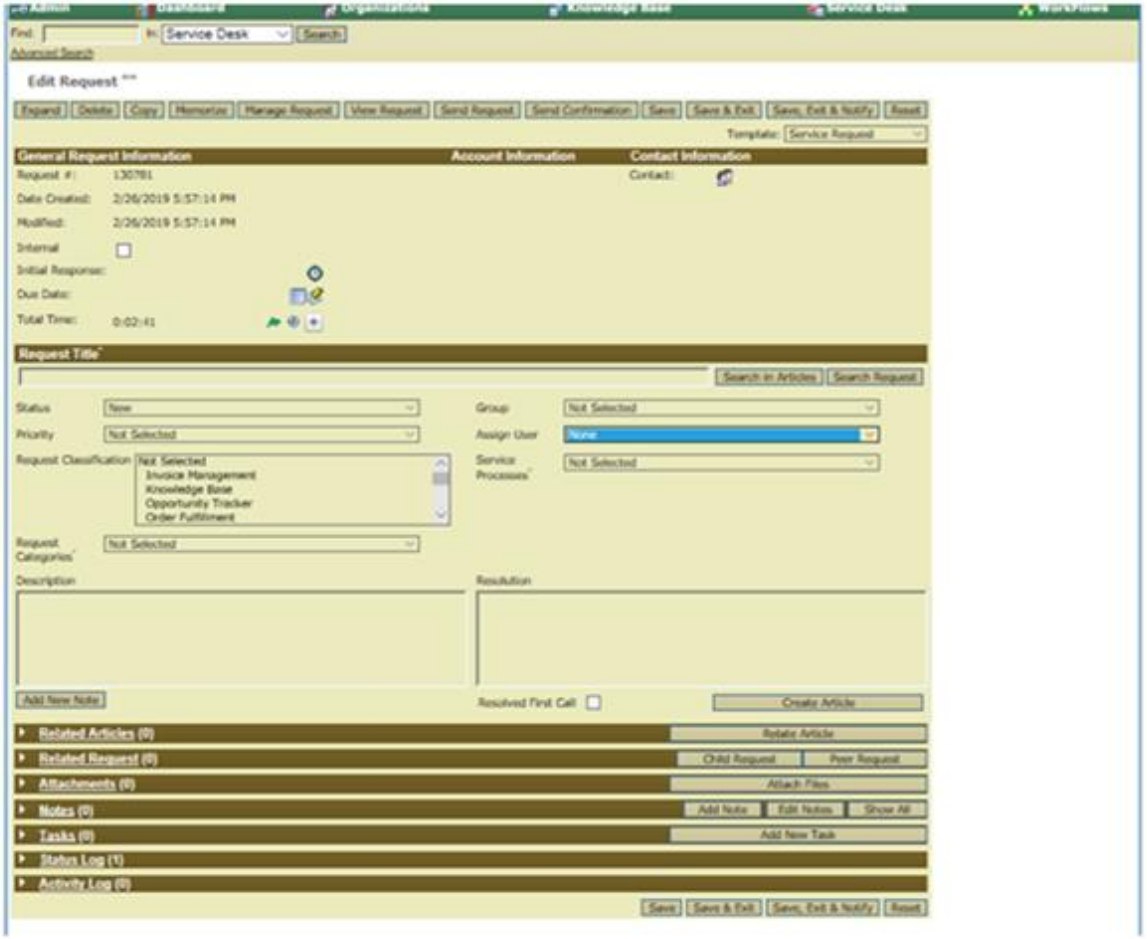
		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SEC 7	**Security - Cybersecurity** **Physical Security** All structures outside the Commission's control that will house components of the ESInet and NGCS shall have security and access-control systems that ensure that only duly authorized individuals can access the areas housing the Commission's systems and network equipment. Any workstations or other equipment connected to, or capable of accessing, the ESInet and NGCS systems shall be housed in secured, access-controlled areas. Any devices, power distribution, and cross-connect panels feeding the cages or rooms housing the Commission's systems similarly shall be protected. Identify any elements that are not under the direct control of the bidder, and a description of the building's security and access-control systems shall be provided.	X			
	Bidder Response: All structures outside the Commission's control that will house components of the ESInet and NGCS are locked, secured with access-control systems that ensure that only duly authorized individuals can access the areas housing the Commission's systems and network equipment. Any workstations or other equipment connected to, or capable of accessing, the ESInet and NGCS systems will be housed in secured, access-controlled areas. NGA 911 utilizes hardened locked caged environments for devices, power distribution, and cross-connect panels feeding the cages or rooms housing the Commission's systems. NGA 911 houses our equipment in secured, access-controlled Data Centers that adhere to Data Center Security Standards: • Access to facilities is only permitted at controlled access points requiring multi-factor authentication designed to prevent tailgating and ensure that only authorized individuals entering our data center. On a quarterly basis, access lists and authorization credentials of personnel with access to data centers housing systems and devices within the system boundary are reviewed by the respective data center Area Access Managers (AAM). • All entrances to data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms if the door is forced open or held open. • Trained security guards are stationed at the building entrance 24x7x365. • If a door or cage within a data center has a malfunctioning card reader or PIN pad and cannot be secured electronically, a security guard is posted at the door until it can be repaired. • In order to provide physical security at the PSAP, NGA 911 recommends a locked cabinet in a secure telecommunications room.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 1	**General Requirements – Network Operations Center (NOC)/Security Operations Center (SOC)** **Centralized NOC/SOC** All services and components deployed and interconnected as part of the solution shall be monitored 24 hours a day, 7 days a week, 365 days a year (24 x 7 x 365) by a centralized Network Operations Center (NOC) and Security Operations Center (SOC). These functions may be in separate buildings or combined in a single building located in the continental United States. **NOC/SOC Interoperability** Contractor shall have the ability to communicate, troubleshoot and connect with other vendors NOCs should there be a different ESInet and NGCS provider. In addition the Contractor shall interface with the NOCs that support the regions throughout the state. This shall include ebonding of the ticket systems to support transparency throughout the troubleshooting process. **NOC/SOC Operations Model** Provide documentation including organizational structure and procedures that describe bidder's 1. NOC/SOC operations model; 2. Continuity Of Operations Plan (COOP); 3. problem and change management systems; 4. reporting system; 5. escalation plan; and, 6. conformance with best practices (Information Technology Infrastructure Library (ITIL) or equivalent methodology)) for service-delivery management. The Contractor shall confirm the requirement compliance of any interconnected network utilized by the Contractor not previously identified to the Commission.	X			
	Bidder Response: **Centralized NOC/SOC** The NGA 911 solution, services, and components deployed and interconnected as part of the solution will be monitored 24x7x365 by a centralized Network Operations Center (NOC) and Security Operations Center (SOC). NGA 911 offers a fully managed service. These administrative and support services include: • 24x7x365 Help Desk with NOC services • 24x7x365 SOC services • 24x7x365 Software support, • 24x7x365 Network monitoring and Security • 24x7x365 Administrative Support • Training Management Information Services • 24x7x365 Technical Support • 24x7x365 Maintenance				

	The above services are provided through the NGA 911 NOC which operates at Tier I and is E-bonded into our Tier II and Tier III support teams. **NOC/SOC Interoperability** The NGA 911 SOC/NOC trouble ticketing systems are electronically bonded (e-Bonding) with all service providers supporting the ticketing system. The e-Bonding of ticketing systems allows near real-time notification of issues, status, and provides tracking or sharing of information between the SOC/NOC and the supplier during an outage and the restoration processes. The SOC/NOC is responsible for communicating this information to the State and the PSAP. NGA 911 will use our system to communicate and troubleshoot with other vendor NOCs if there should be a different ESInet or NGCS provider. Example Reports from the Incident Management System:

NGA 911 Incident Management System

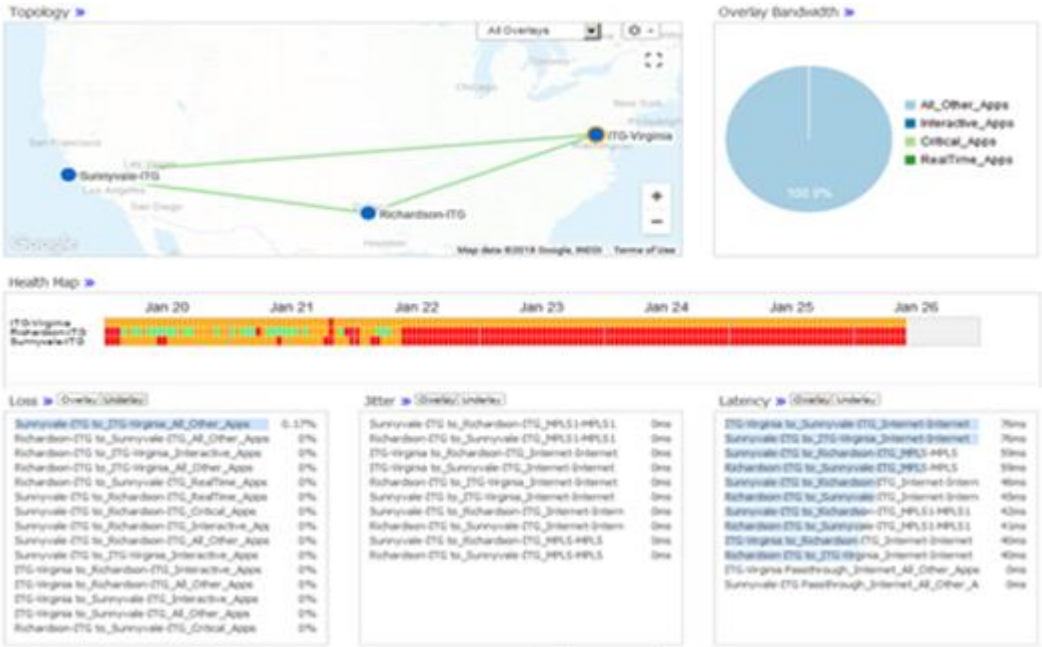


	NOC/SOC Operations Model The following is a description of the NGA 911 NOC/SOC operations model, continuity of operations (COOP) plan, problem change management systems, reporting systems, escalation plan, and conformance with best practices for service delivery management: 1. NOC/SOC operations model - The NGA 911 NOC/SOC is a 24x7x365 monitored facility dedicated to oversight and notification of the State's solution. Our NOC is staffed with trained Tier 2 and Tier 3 Technicians to triage, notify, and adhere to industry-standard processes. 2. Continuity Of Operations Plan (COOP) - The NGA 911 NOC/SOC operations model, continuity of operations (COOP) plan, problem change management systems, reporting systems, escalation plan, and conformance with best practices for service delivery management is described below. **Centralized Management** Configuration management: Controls, optimizes, administers and orchestrates the ESInet from a prime and a backup location. Updates and changes are pushed from centralized management to the network sites for application policy handling procedures, site and network configuration, traffic and security management. Zero-touch provisioning: Allows new sites to be added by simply installing a controller node edge that links the LAN to the WAN. Once the device is installed and connected to the Internet, the configuration information is pushed from centralized management to the CPE and the site becomes part of the network. Security updates: Manages all security policies and patches from centralized policy management. Updates are simultaneously pushed to all sites. Real-time monitoring: Provides a quick and easy way to monitor real-time traffic. Specific details about applications, connectivity paths, locations and network statistics are used to improve network efficiency and quality of service. **Policy Management** NGA 911's Managed service supports QoS, security, and business priorities for all connected sites. Based on customer provided information, NGA 911 will define logical/virtual WAN overlays that reflect application QoS requirements needed. Policies can set minimum and maximum bandwidth limits on the egress traffic per traffic class, to ensure no single application consumes all of the WAN bandwidth. Ingress shaping can be set to ensure that low-priority traffic does not override higher priority traffic.

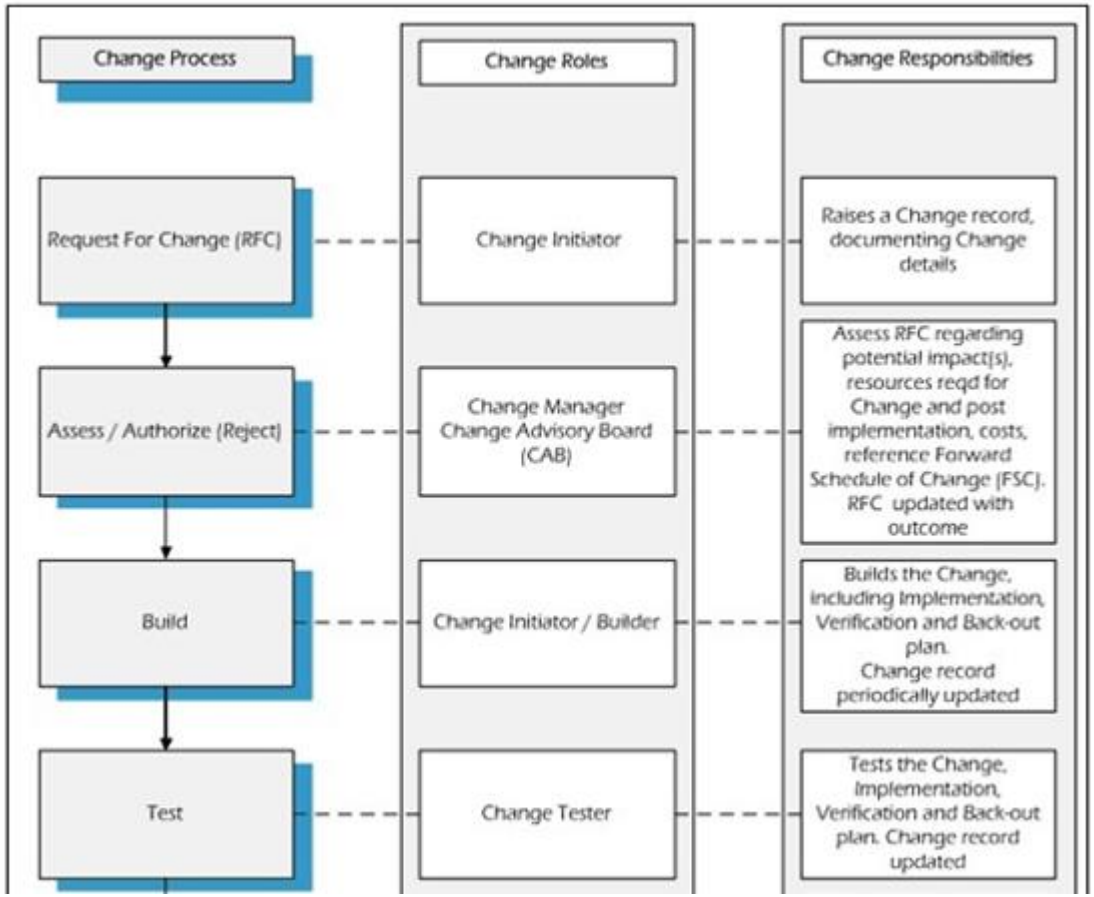
Business intent overlays managed application groups (VOIP, guest Wi-Fi, credit card processing) based on application QoS, SLAs, topology, security policies, and priorities for different applications based on business requirements. Automatically mapping of applications to appropriate overlay optimizes traffic routing decisions and ensures application consistency across the ESInet.

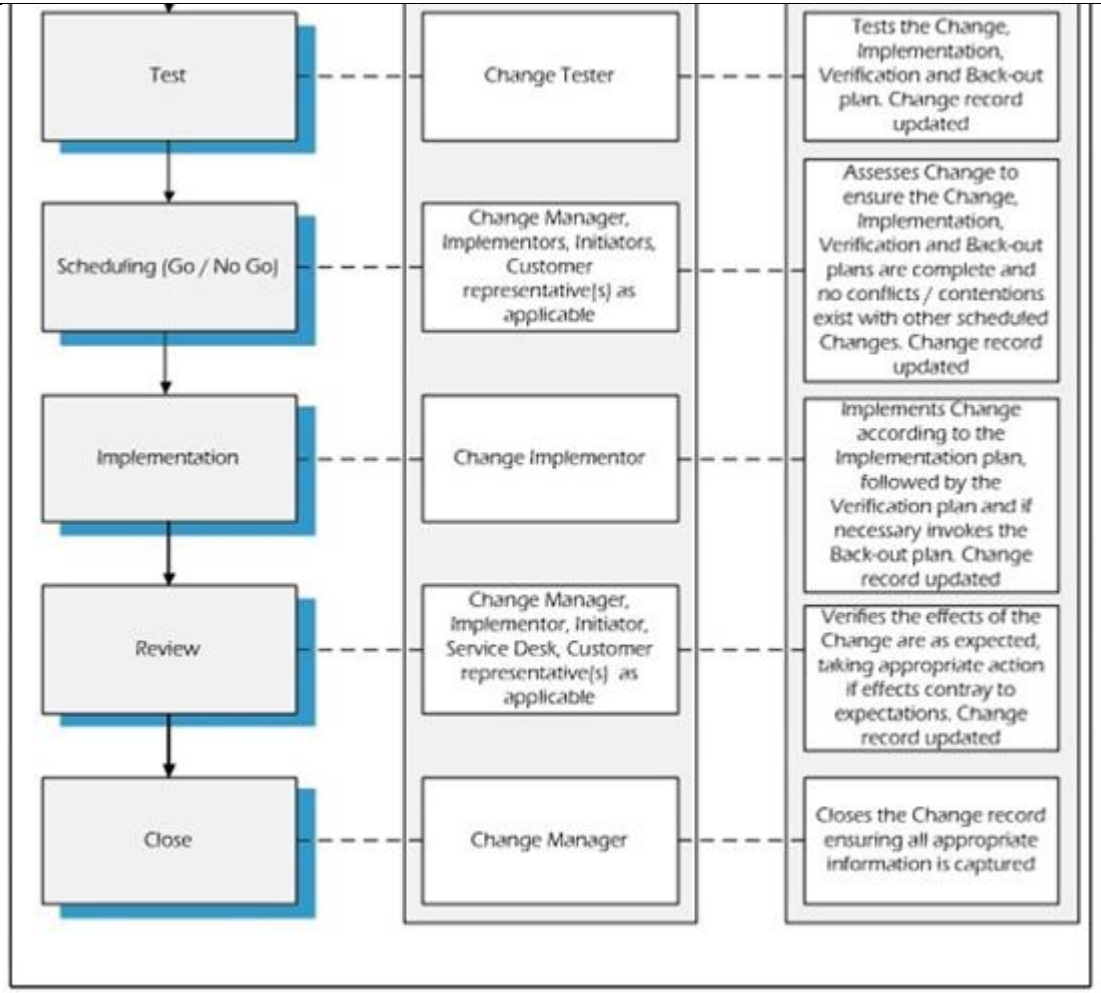
Network Visibility

NGA 911 offers a read-only dashboard and reports for each site including service status, network performance, and other statistics.



3. Problem and change management systems - The NGA 911 change management process follows the ITIL change management process. Below is a Reporting Systems diagram of NGA 911's Change Management Process:


Change Process
Change Roles
Change Responsibilities
Request For Change (RFC)
Change Initiator
Raises a Change record, documenting Change details
Assess / Authorize (Reject)
Change Manager Change Advisory Board (CAB)
Assess RFC regarding potential impact(s), resources reqd for Change and post implementation, costs, reference Forward Schedule of Change (FSC). RFC updated with outcome
Build
Change Initiator / Builder
Builds the Change, including Implementation, Verification and Back-out plan. Change record periodically updated
Test
Change Tester
Tests the Change, Implementation, Verification and Back-out plan. Change record updated



The NGA 911 Change Management System logs all change requests, both from users and those automatically generated. The NGA 911 system interfaces with the Incident Management System for correlation of changes and outages.

	The NGA 911 Web-portal will provide the State Program Manager with the ability to review proposed change requests and the client approval process. NGA 911 will provide monthly reports detailing change tickets opened, resolved, and pending. The NGA 911 Change Management Process is as follows: 1. Initiate a Request For Change (RFC): A request for change can be initiated by opening a Request For Change ticket through the Administrative Portal. This portal allows for the attachment of support documentation. The RFC system will automatically assign an RFC number to the ticket. 2. The RFC will notify all predefined stakeholders (Change Management Board) of the opened ticket for change. 3. The Change Management Board will review the RFC and provide approval/denial. 4. Once the RFC is approved, the change will be designed/built. 5. Upon completion of the build out the change will be tested. 6. Results of the testing will be reviewed and Project Manager/Project Owner and/or State Manager will provide Go/No Go decision. 7. If Go, implementation will be scheduled 8. Change will be implemented 9. Change will be reviewed immediately to determine if there is a negative impact and the Roll Back Plan needs to be initiated or if the 30-day soak begins. 10. Upon successful implementation and 30-day soak, the approval request will be sent to the Project Manager/Program Manager and/or State Manager. 11. RFC will be closed. All steps in the Change Management Process are logged on the RFC ticket and are available for reporting. 4. Reporting systems - NGA 911 solution provides an Administrative System Portal. The NGA 911 Logging tool provides complete access to all metadata generated from NGCS functional elements, including the ESRP via the Administrative Portal. The NGA 911 Reporting System and reporting services included with the proposed solution offer both canned reports and custom reports. The most common NGA 911 reports include: • Total Call Summary • Number of Text to 9-1-1 • Call answering times • Transfers • Custom reports/AD Hoc reports • Calls per hour • Top busiest hour • Call type by class of service

	• Frequently used ANI • Volume Reports • Answer Time Reports • Class of Service • Wireless Carrier • Phase I vs Phase II Comparison • Tower/Cell Sector Reports • Network Reports • Dashboards Additional NGA 911 reports include: • Ring-time statistics • Trunk and line utilization • NGCS element usage volumes • Call processing times between elements • Agent activity • Call transfers • Call conferences • End-to-end call flow analysis

Discrepancy Reports

The ECRF data and system functionality is managed with Discrepancy Reports that conform to STA-010 and include the following information:

- Time stamp of discrepancy submittal
- Discrepancy report ID
- Discrepancy reporting agency domain name
- Discrepancy reporting agent user ID
- Discrepancy reporting agency contact info
- Service or instance in which the discrepancy exists
- Additional notes/comments
- Discrepancy service or database specifics
- Reporting agency's assessment of severity

The response to ECRF discrepancy reports include the following information:

- Responding agency
- Responding agent
- Responding contact
- Estimated response timestamp
- Comment
- Error code

5. Escalation Plan - Manual Escalation
If the PSAP requires escalation during the NGA 911 initial installation and setup process, the PSAP can do the following:

Step 1: Ask to speak to the Technical Support Manager to discuss the issue.

Step 2: Ask to Speak to the Senior Vice President, Operations, if additional escalation is needed.

Step 3: Ask to speak to the Chief Executive Officer if additional escalation is needed.

Automated Escalation Plan

The NGA 911 Dashboard Trouble Reporting Tool has three different automatic escalation types. These three types of escalations are built into the NGA 911 Intelligent Business Rules (IBR) process that are based on predefined trouble ticket criticality. These rules can be updated to meet the City's automated escalation business rules.

- Priority Based Escalation - Automatically assigns staff based on priority of ticket. Low priority tickets are handled by Technical Support staff while high priority tickets automatically escalate to management for review and support.
- Complexity Based Escalation - Engineering levels are created in the IBR to identify more complex tickets and automatically escalate to the more Senior Engineers.
- Service Level Agreement (SLA) Based Escalation - SLAs are built into the IBR that will automatically escalate trouble tickets based on the SLA. The IBR will also proactively assign a ticket to Senior Engineers with a notification to Senior Management when a ticket is approaching a breach of contract.

In addition to service response and service resolution, the escalation matrix helps ensure that available resources are focused on problems that severely affect service. This table defines when additional resources are notified to ensure management is aware of issues and can troubleshoot support. See the following table:

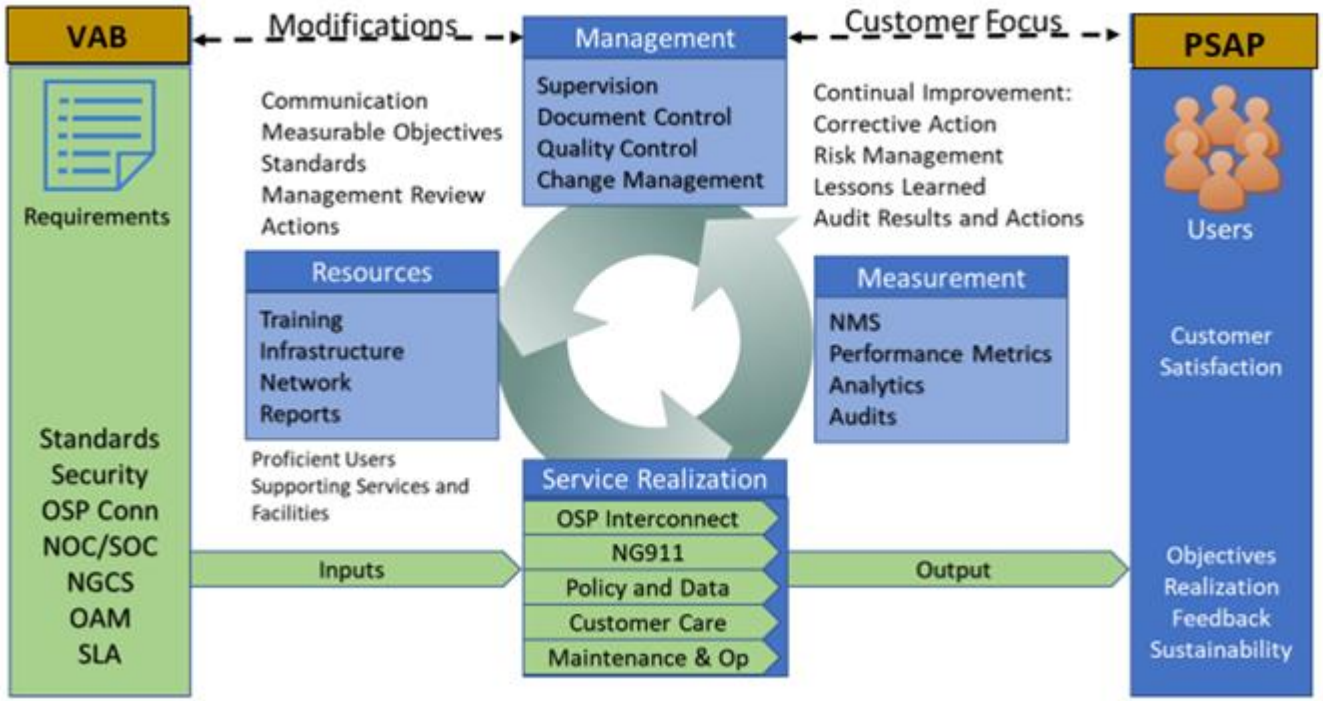
Rank and SLA	Level 1 Critical	Level 2 Major	Level 3 Minor	Level 4 Standard
Response/ Acknowledge	< 15 minutes	< 30 minutes	8 hours	Based on request
Tech on Site (if required)	0-2 hours	2 hours	Next Business Day	Based on request
Escalation Threshold	1 hour	2 hours	48 hours	As needed
Communication Objective	Hourly	Every 2 hours	Daily	As needed

6. Conformance with Best Practices for Service Delivery Management. NGA 911 will confirm the required compliance of any interconnected network utilized by the Contractor not previously identified to the Commission.

As part of our overall Service Delivery Management System (QMS), NGA 911 incorporates the Information Technology Infrastructure Library (ITIL) version 3 service for problem and change management methods and procedures during the initial implementation and ongoing operations of the State's NGCS and ESInet.

NGA 911 adheres to the eight quality management principles: customer focus, leadership, employee involvement, process approach, system approach to management, continual improvement, factual approach to decision making, and mutually beneficial supplier relationships.

A continual improvement process will be integrated throughout the program from commencement to ongoing operations, to assure compliance with requirements, fulfillment of contract performance standards, and the delivery of increasing customer satisfaction.

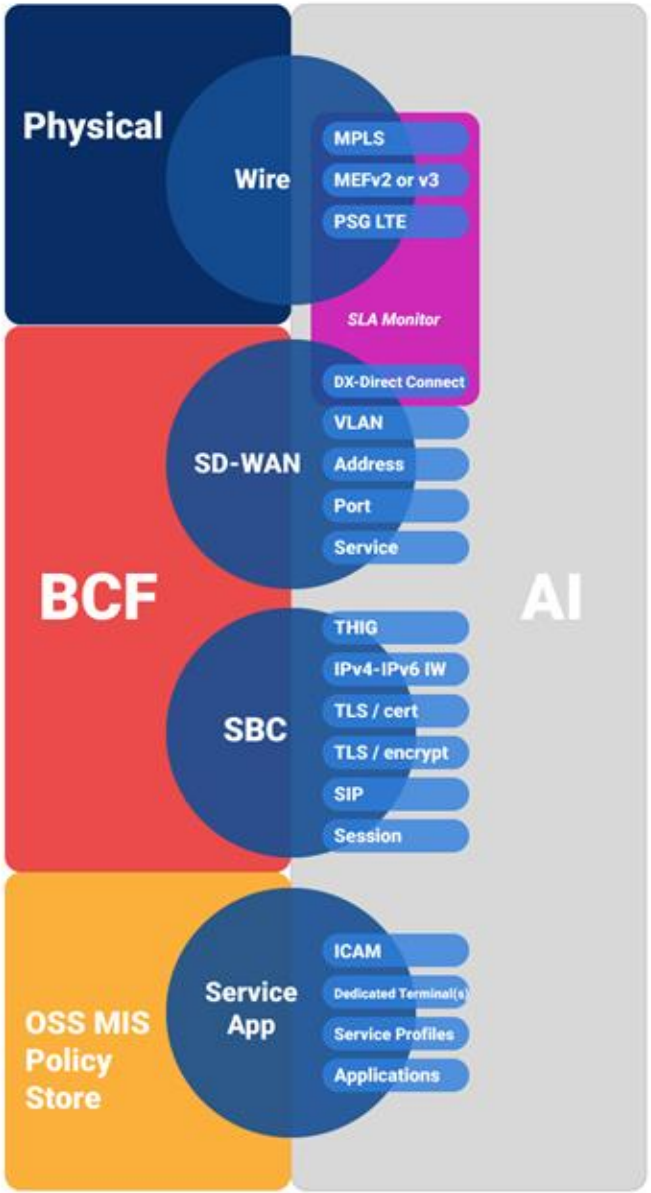


The focal point of our processes is Service Realization in the form of delivering, operating, and maintaining the NGCS and ESInet to the highest possible standards; and continual improvement of services and capabilities for the direct benefit and to the satisfaction of the customer - the first responder community. Keys elements to achieving these goals are, amongst others: (1) meeting State

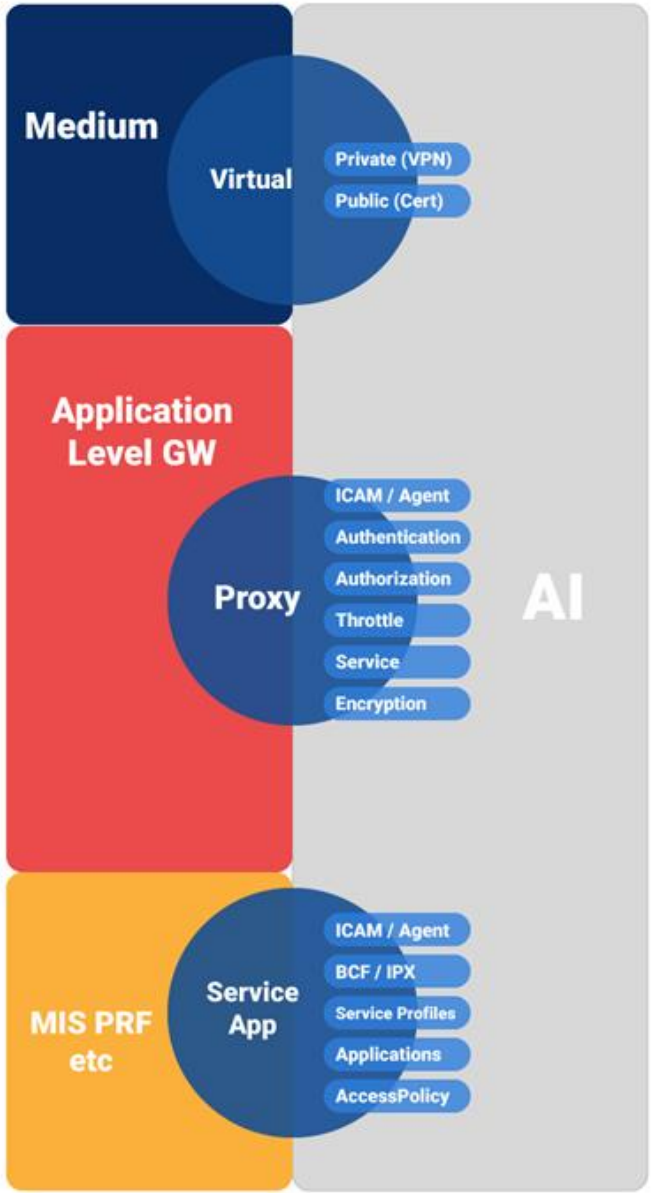
	objectives, (2) a responsive and effective customer care focused approach, (3) consistent maintenance and operations to include continual enhancement of features and capabilities, and (5) a sustainable business model for the State. Service Realization performance, as the focal point of the program, is directly monitored through the quality assurance reporting elements covering critical performance aspects of the contract to achieve the following requirements: (1) demonstrate conformity to the Commission's requirements, (2) ensure conformity to Service Realization requirements, and (3) continually improve the effectiveness of the process and our performance results. Our Management processes drive commitment to continual improvement and effectiveness by: (1) communicating to Partners the importance of meeting contract and statutory requirements, (2) ensuring measurable quality objectives are established, (3) conducting management reviews with meaningful actions, and (4) ensuring the availability of resources to implement an effective Change/Service Management Process. Our Resource Management processes provide for the training and sustainment of the required number of proficient and committed personnel with the requisite qualifications and certifications, and the facilities, infrastructure and work environments to enable personnel to deliver quality maintenance, continually improve services, and enhance customer satisfaction by meeting or exceeding customer requirements.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 2	**NOC/SOC - Remote Connectivity Required** Contractor shall provide any network connectivity required to support proposed NOC/SOC services. Describe any remote connectivity required by the solution including, but not limited to, Virtual Private Network (VPN), phone-home connection, and tech support remote access	X			
	Bidder Response: NGA 911 and authorized users access components, routers, switches, PDUs, functions, services, and other features through two basic means as described below: Internal Access to OSS, Policy Store (PRR) MIS and Reports Certain Operational Support and Policy System Interfaces MUST be held within a NG9-1-1 system. For example, except for the tool used to create the PRRs and provision them in the system, there is no external interface to them. The Policy Routing Rules created and then disseminated by the Centralized Policy Store are strictly classified as sensitive (restricted) as defined in NG-Sec. Other OSS's are tightly regulated on a per-service basis, accessible by SPECIFIC physical hardware with the proper ICAM credentials. For all these Internal cases, FULL BCF to BCF interfaces are enforced.				


Physical
Wire
MPLS
MEFv2 or v3
PSG LTE
SLA Monitor
DX-Direct Connect
VLAN
SD-WAN
Address
Port
Service
BCF
AI
THIG
IPv4-IPv6 IW
TLS / cert
SBC
TLS / encrypt
SIP
Session
ICAM
Service
App
Dedicated Terminal(s)
Service Profiles
Applications
OSS MIS
Policy
Store

	External Access to MIS and Reports Limited external access to the MIS, the NMS, monitoring and reports can be handled by proxies that may grant access to properly credentialed individuals with multi-factor authentication. The proxies themselves will be monitored and limited in their interactions with the NGCS. Such limits include read-only, profile specific authorizations, and access (volume).


Medium
Virtual
Private (VPN)
Public (Cert)
Application Level GW
Proxy
ICAM / Agent
Authentication
Authorization
Throttle
Service
Encryption
AI
MIS PRF etc
Service App
ICAM / Agent
BCF / IPX
Service Profiles
Applications
AccessPolicy

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 3	**NOC/SOC - Network Security Monitoring and Management** **Security Management Solution** The bidder's security management solution shall control access to network resources in accordance with public safety network security best practices such as NIST, NENA and the FCC to prevent sabotage, service interruption (intentional or unintentional) and the compromise of sensitive information. Security management shall comply with security- and data-integrity standards listed in Section V.D.1. Table 1 in the RFP, to monitor users logging into network resources and to refuse access to those who enter inappropriate access codes. The proposed IP network and systems shall support standard security policies that may include the use of firewall rules, Access-Control Lists (ACLs), Virtual Local-Area Networks (VLANs), VPNs, and Transport Layer Security (TLS) protocols to control network traffic and access. The systems shall support the use of software to detect and mitigate viruses, malware, and other attack vectors. Describe how the solution meets or exceeds the above requirement.	X			
	Bidder Response: The NGA 911 security management solution controls access to network resources according to Criminal Justice Information Services (CJIS) Security Policy, version 5.6 or succeeding versions, and with public safety network security best practices such as NIST, NENA and the FCC, to prevent sabotage, service interruption (intentional or unintentional) and the compromise of sensitive information. Security management shall comply with security and data integrity standards listed in Section V.D.1. Table 1 in the RF. Certificates authorize users logging into network resources and to refuse access to those who enter inappropriate access codes. The proposed ESInet supports standard security policies that may include the use of firewall rules, access-control lists (ACLs), virtual routing and forwarding (VRF), VLANs, VPNs, and the TLS and SSL protocols to control network traffic and access. The systems and servers support the use of software to detect and mitigate viruses, malware, and other attack vectors. The NGA 911 solution provides details that exhibit security information and event management (SIEM) compliance to include correlation of events and the ability to monitor in real-time. NGA 911 maintains a living security document known as the Security Policy Note (SPN) which is the basis of our defense in depth approach to all layers of security. The latest version of the operational SPN is SPN_NGA 911 Security Framework Overview v_f_2020. A CONFIDENTIAL copy of the SPN will be shared and discussed with the State as part of contract negotiations. The intention of NGA 911 consistent with our QMS is to align the SPN Security Framework to the requirements of the Commission and the State's CIO Office or practices.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 4	**NOC/SOC - Connected Systems Compliance** Any system that connects to an IP network shall be required to comply with listed standards in Table 1, including security standards, and demonstrate compliance through an initial and recurring audit. **A. Security Reports and Recommendations** Contractor shall provide, within 30 days of the end of each calendar month, security summary reports and recommended improvements on a monthly basis (at a minimum), including incidents and incident response; building, facility, and network access reports, including failed attempts; and updates or changes to security systems and software. All related data shall be retained for the period of the contract and provided to the Commission electronically at the end of the contract. Describe how the solution meets or exceeds the above requirement.	X			
	Bidder Response: NGA 911 will comply with all listed standards in Table 1, including security standards. NGA 911 will demonstrate compliance through initial and recurring audits. NGA 911 will provide within 30 days of the end of each calendar month: • Security Summary Reports • Recommended Improvements • Incidents and incident response • Building, facility and network access reports including failed attempts • Updates or changes to security systems and software All data will be retained for the period of this contract and will be provided to the Commission electronically at the end of the contract or upon request. NGA 11 will allow for security audits with reasonable notice of 30 calendar days or as agreed to with the State when requested by the State and at the cost of the State including but not limited to: 1. Whitelisted scanning and manual testing of the application only, with application credentials equal to the least privileged role within the application 2. Manual verification of scan results with the same credentials 3. Manual testing of the application for vulnerabilities 4. Internal audits and system scans for vulnerabilities on a quarterly basis for the first year following deployment of the first PSAP and annually for the remainder of the contract and report findings to the State with recommendations for improvements				

	NGA 911 will comply with all applicable FCC outage and notification rules throughout the term of the contract. NGA 911 has a Real Time Network Outage Monitoring and Reporting Dashboard that covers all of the NGCS functional elements (FE) and ESInet. NGA 911's Dashboard enables real time monitoring by all stakeholders of all 9-1-1 traffic and all NG9-1-1 trunks to ensure that SLAs are being met. The service status can be displayed geographically and be tied to the SLA using color coding by type of incident. Additionally, the Dashboard is connected to our real time communication console that provides immediate alerts and escalation to all stakeholders with transparent access to issue tracking and resolution; further, the Dashboard is connected to our real time business intelligence, analytics, and data warehouse for immediate reporting. The Dashboard and its associated transparency are vital to project success for all stakeholders because issues must be identified immediately so that a strong knowledge base can be created to operate this new NG9-1-1 solution for the state. NGA 911 will provide a monthly Security Status Report to the State. The Status Report will provide essential information regarding the security posture of the ESInet as well as the effectiveness of the control currently deployed for network, facilities, and core services including incidents and incident response, attempts failed or successful to access network, facilities, or core services. NGA 911 will provide reports of incidents, including regularly scheduled monthly reports. The reports will include at a minimum all performance items identified below regarding NGA 911's SLA solution: 1. Tickets opened by Incident Number 2. Tickets closed by Incident Number 3. Affected location or routing element 4. SIL of incident 5. Incident type 6. Incident duration 7. Resolution

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 5	**NOC/SOC – Connected Systems Compliance** **A. Support for Similar Solutions** Provide details concerning how bidder provides security monitoring and management for similarly deployed production solution. Provide details, including drawings, which explain how the proposed solution meets or exceeds the above requirements.	X			

Bidder Response:

The SOC ensures that the network is protected against cyber-attacks and maintains security elements of confidentiality (protection of information), integrity (trustworthiness of the information passed around in the network), and availability (preventing bad actors from blocking access to legitimate network users.)

The SOC ensures proper operation and monitoring of firewalls and intrusion prevention systems. The SOC also performs an "internal affairs" function: security information and event management (SIEM) to ensure that internal personnel are not causing a security breach. Finally, the SOC analyzes the "access logs" for security threats and inappropriate patterns of behavior. These logs are the history showing which internal personnel performed which actions on which components and what time.

The SOC manages the Security Incident Response Program for the NGCS that is tailored to the unique operating environment. The IR plan determines the speed and efficacy of a response to a crisis through a methodical and coordinated series of steps composed of Response Actions (RAs) aimed at resolving a reported incident. This comprehensive and systematic approach to security events protects the NGCS, ensuring that it remains resilient during an incident. The IR Program is structured to identify, report, coordinate, and resolve incidents in accordance with the incident response framework that consists of six phases, as shown in the figure.

Timeline of Events	**Time-based record denoting what activities or efforts occurred during incident handling**

Agency SART & Incident Handler	**Name of affected agency that is reporting the incident. Name and contact information of the incident handler should be noted (i.e., business email & phone)**	
Incident Severity Impact	**Impact on network denoting the severity of the incident (High, Medium, Low)**	
Incident Security Impact	**Impact on relevant security context of a system (i.e., Confidentiality, Integrity, Availability)**	
Incident Status	**Status of the incident (Open, Closed)**	
Incident Category	**Categorization of the incident denoting the level of actionable effects on the system**	
Incident Tracking Number	**(For example, Unauthorized Access (Intrusion) – Category 1)**	

Source & Destination Systems Involved	**Tracking mechanism assigned to the incident by a central ticketing system where security teams can reference the incident and its up-to-date status**
Affected/Impacted Usernames	**System descriptors by IP address, MAC address, Hostnames, Web URL address links or functional role**
Analysis Results	**Concise description of initial investigation efforts. The analysis should include relevant technical details pertaining to the incident.**

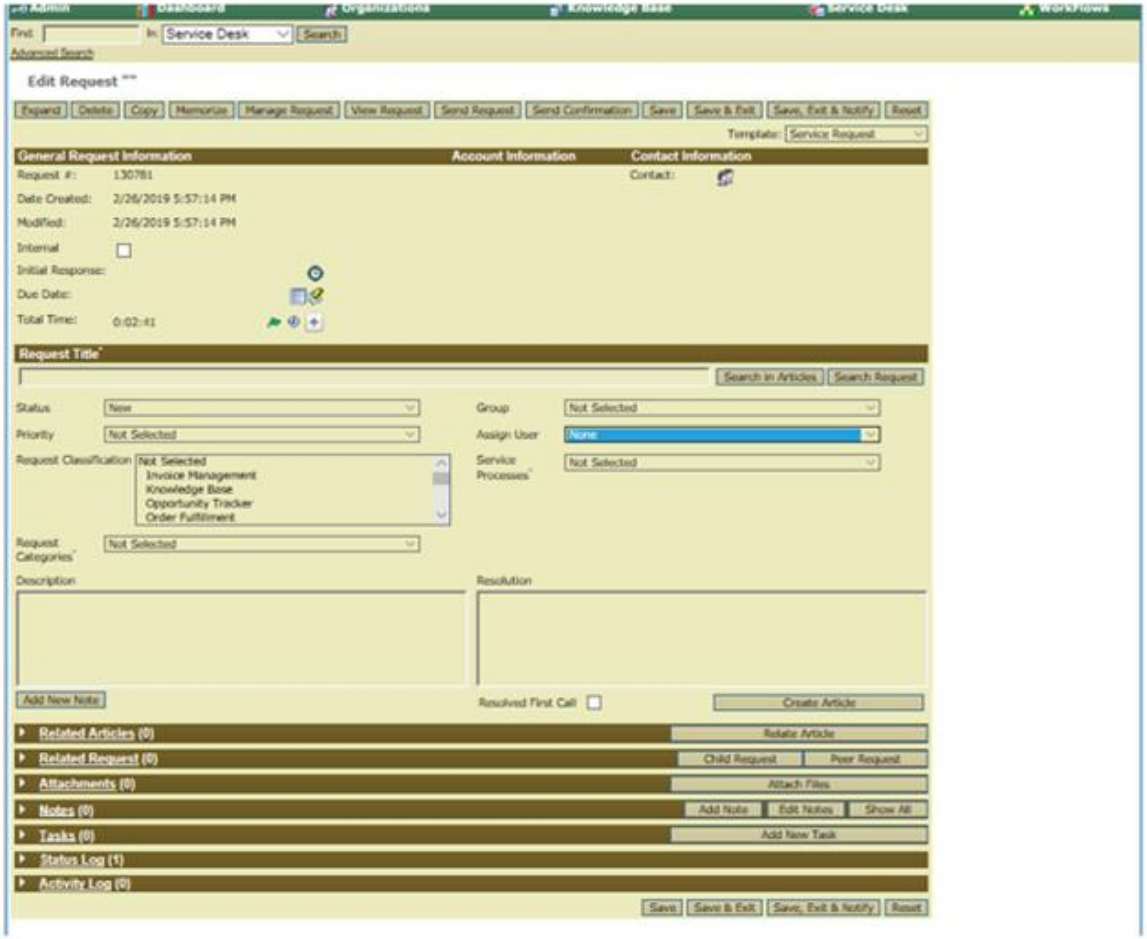
Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 6	**NOC/SOC - Physical Access Monitoring and Management** **Physical Access Monitoring and Reporting** Contractor shall track and log all physical access to structures housing IP network components serving the Commission or have the capability to obtain access logs for structures not under immediate control of the bidder. Reports may be requested and shall be made available for review upon request. All related data shall be retained for the period of the contract and provided to the Commission electronically at the end of the contract. Provide a detailed explanation of bidder's processes and procedures for logging physical access to ESInet /NGCS components, and how the bidder's solution generates the required reports.	X			
	Bidder Response: Physical access to all data centers housing IT infrastructure components is restricted to authorized data center employees, vendors, and contractors who require access in order to execute their jobs. Access to facilities is only permitted at controlled access points requiring multi-factor authentication designed to prevent tailgating and ensure that only authorized individuals enter our data center. On a quarterly basis, access lists and authorization credentials of personnel with access to data centers housing systems and devices within the system boundary are reviewed by the respective data center Area Access Managers (AAM). All entrances to data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms if the door is forced open or held open. Trained security guards are stationed at the building entrance 24x7x365. If a door or cage within a data center has a malfunctioning card reader or PIN pad and cannot be secured electronically, a security guard is posted at the door until it can be repaired. NGA 911 will make available to the State all reports for review as part of the problem management reporting.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 7	**NOC/SOC - Incident Management System** The bidder's incident management system shall log all support requests, both from users and those automatically generated. 1. Provide examples of monthly reports detailing tickets opened, pending, resolved, and closed. 2. Provide a matrix outlining Service Impact Levels in a detailed response, to include notification times and response times.	X			
	Bidder Response: 1. The NGA 911 Incident Management System (IMS) is a web-based solution. The IMS generates an incident that remains open and in queue until it is resolved. The IMS logs all support requests, both from users and those automatically generated through network and system monitoring tools. The NGA 911 IMS allows for incident management capabilities for trouble ticket management. It keeps a log of troubleshooting and/or research performed along with support requests from the PSAP, users, and ones the system automatically generates. The Web-Portal is available 24x7x365. This allows the PSAP or the State to submit and check the status of incidents, view notes, and history as required. The PSAP or State can view open, resolved, and pending tickets along with the details ticket. A sample report has been provided.				

NGA 911 Incident Management System



Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

Request: #	Request: Problem/Issue	Request: Status	Request: Completed	Request: Added
		Closed		
130193	New Heat Ticket: 00408559	Closed	2/18/2019 13:46	2/4/2019 11:51
130206	New Heat Ticket: 00408188	Closed	2/18/2019 13:45	2/5/2019 14:18
130207	New Heat Ticket: 00408147	Closed	2/18/2019 13:45	2/5/2019 14:20
130208	New Heat Ticket: 00408176	Closed	2/18/2019 13:44	2/5/2019 14:20
130209	New Heat Ticket: 00408118	Closed	2/18/2019 13:44	2/5/2019 14:22
130210	New Heat Ticket: 00408116	Closed	2/18/2019 13:44	2/5/2019 14:24
130211	New Heat Ticket: 00408094	Closed	2/18/2019 13:43	2/5/2019 14:26
130212	New Heat Ticket: 00407925	Closed	2/11/2019 14:45	2/5/2019 14:33
130213	New Heat Ticket: 00407445	Closed	2/11/2019 15:05	2/5/2019 14:41
130214	New Heat Ticket: 00407482	Closed	2/18/2019 13:43	2/5/2019 14:41
130215	New Heat Ticket: 00407266	Closed	2/18/2019 13:42	2/5/2019 14:43
130216	New Heat Ticket: 00408152	Closed	2/11/2019 14:51	2/5/2019 15:01
130218	New Heat Ticket: 00404922	Closed	2/18/2019 13:41	2/5/2019 15:18
130219	New Heat Ticket: 00407915	Closed	2/18/2019 13:40	2/5/2019 16:28
130228	New Heat Ticket: 00408287	Closed	2/18/2019 13:39	2/6/2019 13:29
130237	New Heat Ticket: 00408876	Closed	2/18/2019 13:38	2/7/2019 10:28
130243	New Heat Ticket: 00408817	Closed	2/18/2019 13:37	2/7/2019 15:17
130244	New Heat Ticket: 00408404	Closed	2/18/2019 13:37	2/7/2019 15:21
130245	New Heat Ticket: 00408106	Closed	2/18/2019 13:37	2/7/2019 15:36
130247	New Heat Ticket: 00406562	Closed	2/18/2019 13:36	2/7/2019 15:48
130249	New Heat Ticket: 00408843	Closed	2/18/2019 13:35	2/7/2019 16:59
130250	New Heat Ticket: 00408762	Closed	2/18/2019 13:35	2/7/2019 16:59
130252	New Heat Ticket: 00408828	Closed	2/18/2019 13:34	2/8/2019 9:06
130253	New Heat Ticket: 00408821	Closed	2/18/2019 13:34	2/8/2019 9:17
130256	New Heat Ticket: 00406927	Closed	2/18/2019 13:34	2/8/2019 10:46
130323	New Heat Ticket: 00409667	Closed	2/18/2019 13:32	2/15/2019 14:31
130326	New Heat Ticket: 00409371	Closed	2/18/2019 13:32	2/15/2019 14:43
130103	New Heat Ticket: 00406541	Closed	2/13/2019 17:34	1/24/2019 10:24
130104	New Heat Ticket: 00407549	Closed	2/11/2019 12:39	1/24/2019 10:40
130105	New Heat Ticket: 00407342	Closed	2/18/2019 13:50	1/24/2019 10:50
Request: # Count: 30				
		Open		
130114	New Heat Ticket: 00403115	Open	2/11/2019 14:05	1/24/2019 11:38
130102	New Heat Ticket: 00407182	Open	2/11/2019 12:39	1/24/2019 10:07
Request: # Count: 2				
Report Count: 32				

2. Sample matrix outlining Service Impact Levels.

Rank and SLA	Level 1 Critical	Level 2 Major	Level 3 Minor	Level 4 Standard
Response/ Acknowledge	< 15 minutes	< 30 minutes	8 hours	Based on request
Tech on Site (if required)	0-2 hours	2 hours	Next Business Day	Based on request
Escalation Threshold	1 hour	2 hours	48 hours	As needed
Communication Objective	Hourly	Every 2 hours	Daily	As needed

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 8	**NOC/SOC - Change Management System** **Change Management Review System** Describe bidder's change management system and the ability to provide the Commission's program manager and designated PSAP representatives with the ability to review proposed change requests and the client approval process. The Contractor shall provide monthly reports detailing change tickets opened, pending, resolved, and closed.	X			
	Bidder Response: The NGA 911 Change Management system will be available to authorized personnel including the Commission Manager and designated PSAP representatives through the NGA 911 Web-Portal. All change requests will be entered into the IMS and assigned an Event ID. All coordination, communications, impacted stakeholders, and client approval will be logged on the Event ID. All Events in the IMS are stored and maintained for historical information for the term of the contract. The credentialed State personnel, its representatives, and PSAPs will have access to the data through the Web-Portal, however, NGA 911 will also provide copies of the data to the State on request and at the end of the contract. NGA 911 will provide monthly reports detailing change tickets opened, pending, resolved, and closed. NGA 911 will provide Change Management reports for system and other changes. These reports are also available to the State through the Web-Portal. See sample report and Change Request Form:				

NGA 911 Change Request Form Template

Project Name	Name of project		
Requested by	Name of requestor	**Date**	Date request was raised
Request No	Request Number	**Name of Request**	Brief name of request
Change Description	Description of the change		
Change Reason	Give the justification for the change		
Impact of Change	Specify the impact in terms of cost, budget, schedule, and other projects		
Proposed Action	Does the project Manager propose this change is accepted/rejected and why		
Status	In review	Approved	Rejected
Approval Date	The date the change was approved or rejected		
Approved By	Who approved the change		

Change Management Report

Change Management Status Report

Project Name: Sample **Report Date:** 2/15/2020

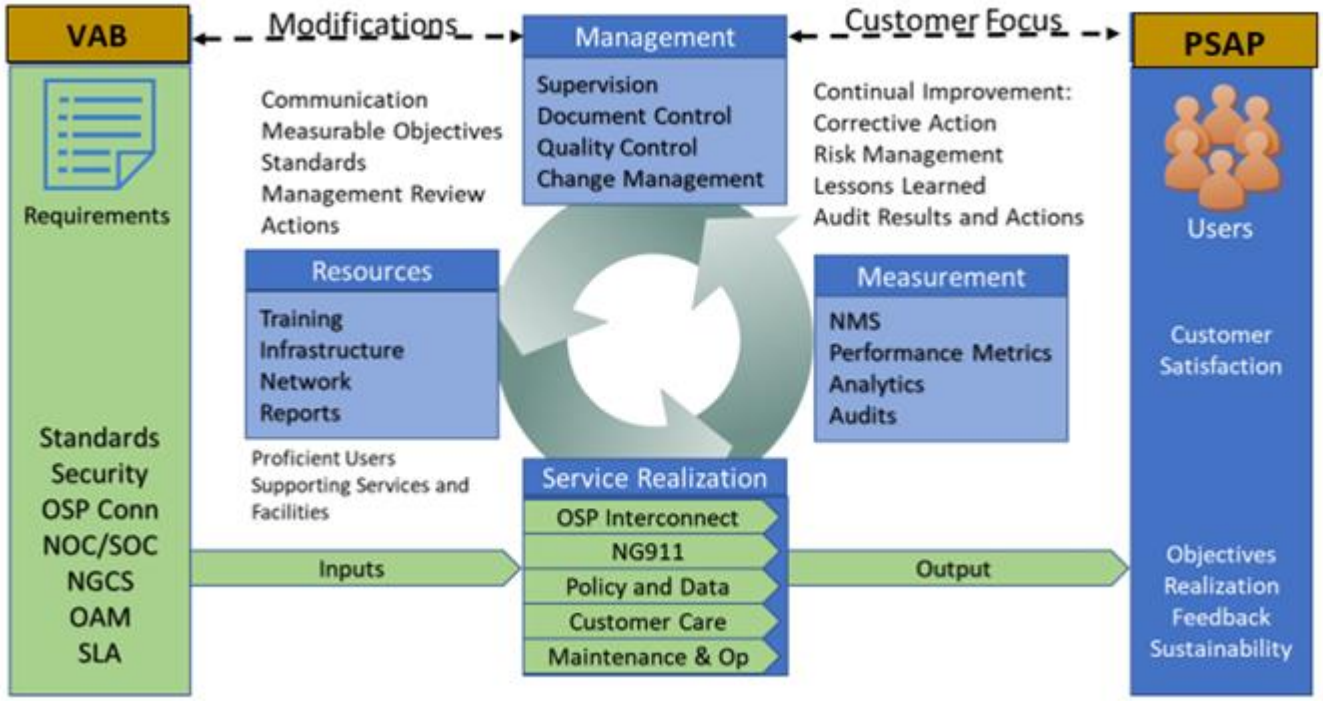
Report From: 2/1/2020 Report To: 2/14/2020 **Period:** Month

Filters:

Call Type: NA
Abandon: NA

Date	Event ID	Type	Description	Approval Status	Owner	Due Date
2/1/2020	12459	Risk	Technical Risk – Change requested to ESInet Design	Pending	Ed Vea	2/25/2020
2/5/2020	13672	Decision	A change to a Dash Board View has been requested	Approved	Mark LeMonn	3/1/2020

NGA 911 incorporates the Information Technology Infrastructure Library (ITIL) version 3 service for problem and change management methods and procedures during the initial implementation and ongoing operations of the NGCS and ESInet. The NGA 911 documented Management Process includes a process to request change, completing Change Management forms detailing the description, reason and impact of change, activity, test plans, backout plans, and specific list of named systems, applications, and/or hardware to be affected by the change, and obtaining the Customer's approval. The Change Requests are discussed and approved in a Change Control Board Meeting. If the change involves other vendors, those vendors are included in the Change Control Board Meetings. NGA 911 has a process to communicate the requested change with the vendor. Approved changes are implemented and then the outcome of the change is presented at a subsequent Change Control Board Meeting. Routine changes such as system updates, patches, etc. are implemented according to customer maintenance windows and update and patch schedules.



NGA 911 adheres to industry standard processes including Information Technology Infrastructure Library (ITIL) workflows.

Any additional documentation can be inserted here:

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

NOC/ SOC 9	**NOC/SOC - Change Management System** **A. Change Management Tools** Provide detailed descriptions of any other tools bidder intends to use to provide access to the change management system, such as web portals and client software.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The NGA 911 system is available through a web browser. The Commission and PSAPs can use laptops, tablets, desktop computers, and mobile devices to access the Change Management System.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 10	**NOC/SOC – Change Management System** **A. Change Testing and Training Environment** A non-production NGCS replica, test lab, or similar system shall be established to test, and exercise proposed upgrades, third-party interfaces, and applications prior to release in live production. This system also could be leveraged for training purposes. Provide detailed descriptions of how the solution satisfies this function in the change management process.	X			

Bidder Response:

NGA 911 will collaborate with the State to plan all necessary system testing for each service, component, function, application or piece of equipment comprising the proposed solution in our non-production lab. System testing of any new implementations, third-party interfaces, and applications prior to their release in a live production environment is required in our non-production lab prior to any cutover to full operational status.

<u>Production replica for testing:</u>

All new functions and features are subject to thorough and robust testing in a pre-production environment (i.e. an Illinois dedicated replica test environment). NGA 911 operates a comprehensive ITIL DevOps organization and process for testing in our non-production lab. NGA 911 will conduct comprehensive, complete and thorough testing, adhering to a clearly defined validation process. The State will sign a Certificate of Acceptance (COA) form prior to moving the solution into live day-to-day operations.

NGA 911 runs a number of labs for various R&D, interoperability (IOT), pre-production, and scale testing. For Nebraska, NGA 911 will build a complete instantiation of all the network elements. It is this pre-production network/lab that is used to test first, simulated loads, PSAP, Data Center, NGCS, and OSP connectivity, and then IOT.

All the elements of the production environment will be in place:

1. Data Centers (DCs) including
    - Aggregation Router
    - Carrier and PSAP IXC (interconnect)
    - Dx (AWS Direct Connect)
2. Central Office / Switching Centers
    - LNG
    - TDM IXC
3. NGCS in the Cloud
    - BCF, ESRP, PRF, ECRF, LVF
    - MIS, NMS, Proxies
4. NG Trunks

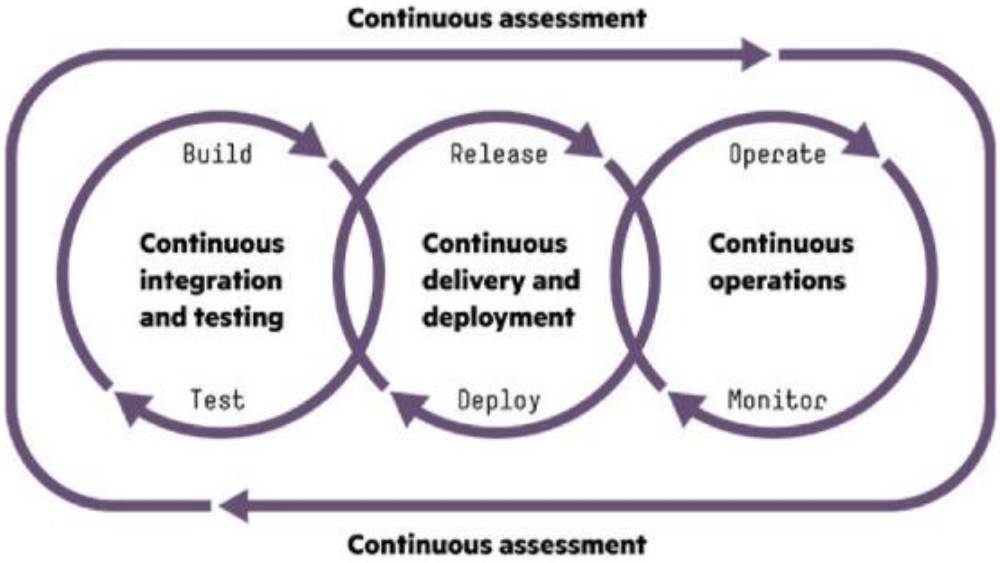
- Between elements (PSAPs, DCs, NGCS, other ESInets, Carriers)
- With appropriate Bandwidth

5. PSAP
   - LPG (as required)
   - BCF

6. SD-WAN endpoint

All the above will be deployed for testing the production environment with a minimum of one (but most likely more) example of each.

Iterative, Continuous Assessment DevOps Process:



	NGA 911 adheres to the continuous assessment model depicted in the diagram above. Build types are characterized as being based on customer needs, on enhancements, and on Operational Necessity. Each type is coded in an Agile manner and integrated into the Test Environment.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 11	**NOC/SOC – Change Management System** **A. Change Management Process** 1. Outline bidder's proposed change management process. The ITIL change management standard methods and procedures are preferred. 2. Include a description of the process for notifying the Commission and affected PSAPs. Notification shall be made no less than ten (10) business days in advance of the change, except in emergency situations, in which case notification shall be provided immediately. 3. Include explanation of solution's Fault, Configuration, Accounting, Performance, and Security (FCAPS) procedures. 4. Provide a detailed explanation describing how the proposed solution meets or exceeds the requirements for the ITIL and FCAPS processes.	X			

Bidder Response:

NOC/SOC – Change Management System Change Management Process

1. As part of our overall Quality Management System (QMS), NGA 911 incorporates the Information Technology Infrastructure Library (ITIL) version 3 service for the implementation of new standards and updated standards. The ITIL also drives NGA 911's change management methods and procedures during the initial implementation and ongoing operations of the State and the PSAPs.

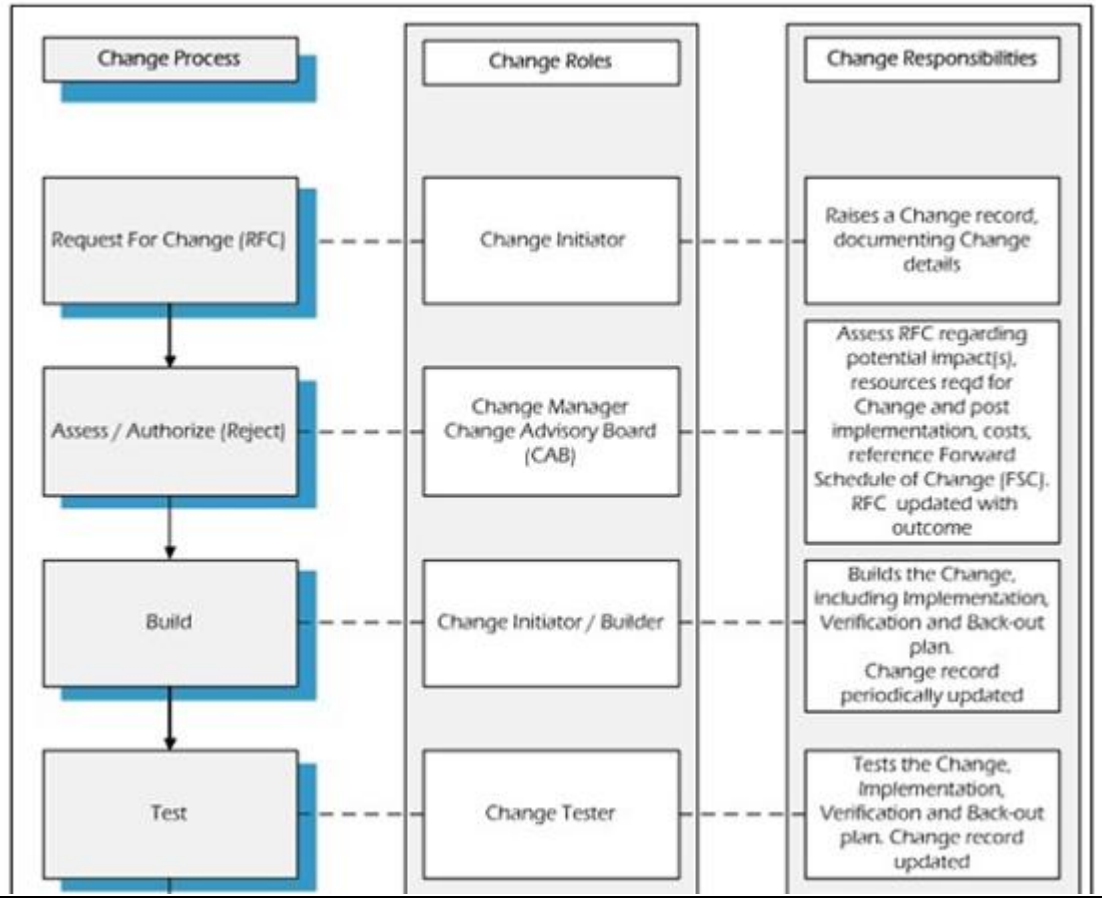
Request for Change (RFC) is submitted to the change management team for validation and approval.

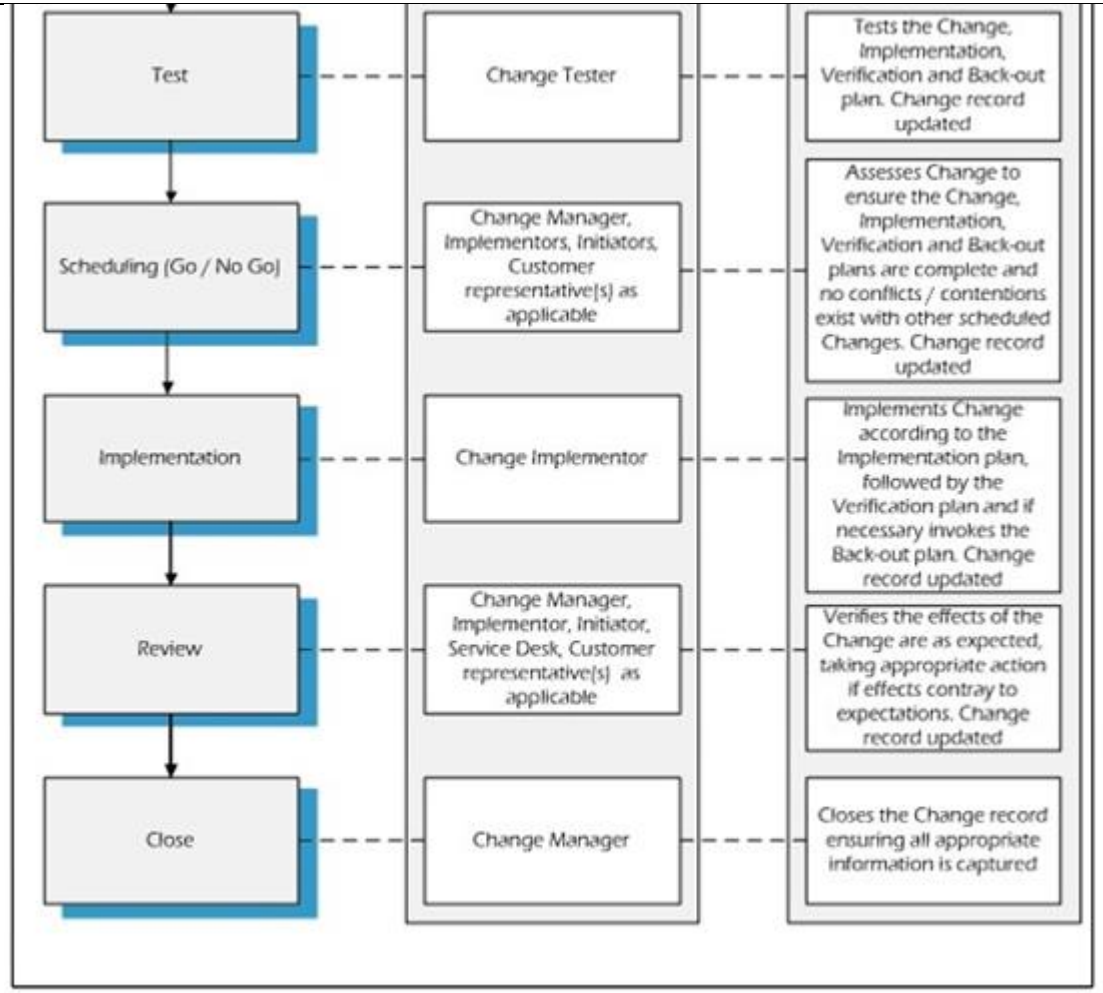
A RFC template is used to record the change

- Reason for change - Justifies why change is needed along with risk/benefit analysis.
- Impact & Risk assessment - Potential Impact and risk are calculated and documented including configuration items..
- Implementation planning - Steps for implementing change that includes project members, timelines and methodology.
- Prioritization - Determine the type of change and prioritize the requests accordingly.
- Scheduling - Check the Release schedule to get an estimated time frame and fix the planned start date and end date
- Roll out plan - Plan out the implementation activities
- Back out plan - Back out plan in case of unexpected setbacks.

The NGA 911 documented Management Process includes a process for defect resolution, request change, completing Change Management forms detailing the description, reason and impact of change, activity, test plans, backout plans, and specific list of named systems, applications, and/or hardware to be affected by the change, and obtaining the State and PSAP's approval. The Change Requests are discussed and approved in a Change Control Board Meeting. If the change involves other vendors, those vendors are included in the Change Control Board Meetings. NGA 911 has a process to communicate the requested change with the

	vendor. Approved changes are implemented and then the outcome of the change is presented at a subsequent Change Control Board Meeting. Routine changes such as system updates, patches, etc. are implemented according to the PSAP maintenance windows and update and patch schedules. 2. The NGA 911 process for notifying the Commission and affected PSAPs is stated below. NGA 911 will notify no less than ten (10) business days in advance of the change, except in emergency situations, in which case notification will be provided immediately.


Change Process
Change Roles
Change Responsibilities
Request For Change (RFC)
Change Initiator
Raises a Change record, documenting Change details
Assess / Authorize (Reject)
Change Manager Change Advisory Board (CAB)
Assess RFC regarding potential impact(s), resources reqd for Change and post implementation, costs, reference Forward Schedule of Change (FSC). RFC updated with outcome
Build
Change Initiator / Builder
Builds the Change, including Implementation, Verification and Back-out plan. Change record periodically updated
Test
Change Tester
Tests the Change, Implementation, Verification and Back-out plan. Change record updated



The NGA 911 Web-portal will provide the Commission with the ability to review proposed change requests and the client approval process. NGA 911 will provide monthly reports detailing change tickets opened, resolved, and pending. The NGA 911 Change Management Process is as follows:

	A. Initiate a Request For Change (RFC): A request for change can be initiated by opening a Request For Change ticket through the Administrative Portal. This portal allows for the attachment of support documentation. The RFC system will automatically assign an RFC number to the ticket. B. The RFC will notify all predefined stakeholders (Change Management Board) of the opened ticket for change. C. The Change Management Board will review the RFC and provide approval/denial. D. Once the RFC is approved, the change will be designed/built. E. Upon completion of the build out the change will be tested. F. Results of the testing will be reviewed and Project Manager/Project Owner and/or State Manager will provide Go/No Go decision. G. If Go, implementation will be scheduled H. Change will be implemented I. Change will be reviewed immediately to determine if there is a negative impact and the Roll Back Plan needs to be initiated or if the 30-day soak begins. J. Upon successful implementation and 30-day soak the approval request will be sent to Project Manager/Program Manager and/or State Manager. K. RFC will be closed. 3. NGA 911's solution aligns with the fault, configuration, accounting, performance, and security (FCAPS) procedures by using tools to recognize, isolate, correct and log faults that occur in the network. Furthermore, we use trend analysis to predict errors so that the network is always available. <u>Fault</u>: When a fault or event occurs, notification is sent to collect information about network devices. Our management station makes the network administrator aware of problems (by email, paging, or on-screen messages), allowing appropriate action to be taken.

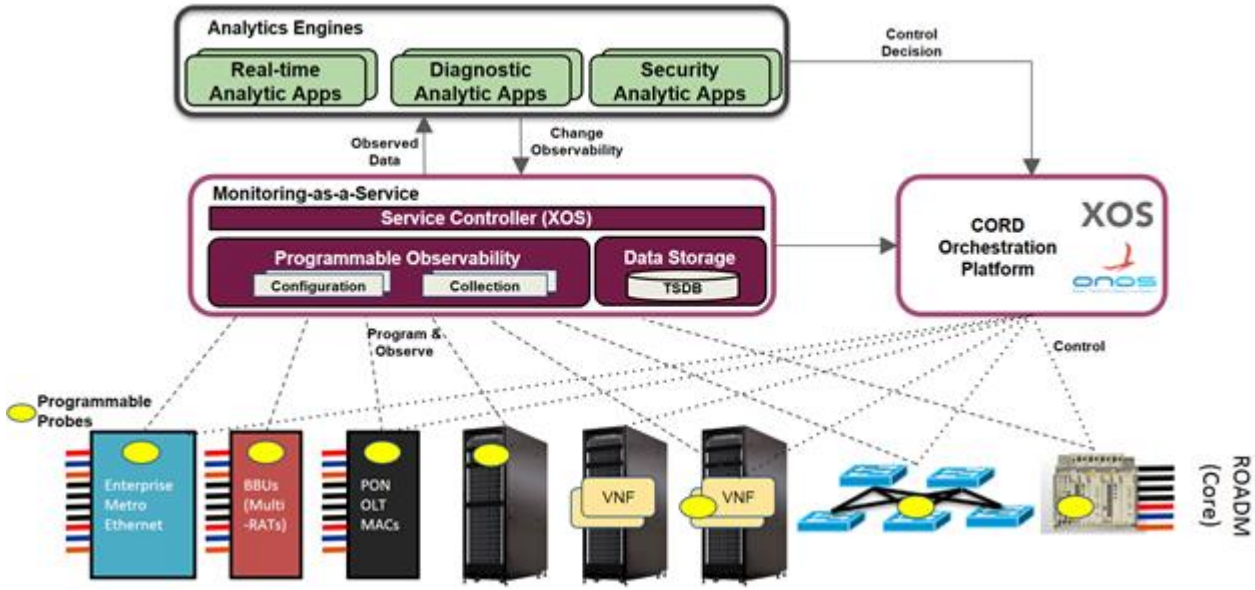
	Configuration: We gather and store configurations from network devices (this can be done locally or remotely) and track all changes made to network hardware and software. Accounting management: We track network utilization information, such that individual users, departments, or business units can be appropriately billed or charged for accounting purposes. Performance management: Enables us to prepare the network for the future, as well as to determine the efficiency of the current network, for example, in relation to the investments done to set it up. The network performance addresses the throughput, network response times, packet loss rates, link utilization, percentage utilization, error rates and so forth. Security management: Through Security management we control access to assets in our network. NGA 911's Data security is achieved mainly with authentication and encryption. We not only ensure the network environment is secure, but also gather security-related information and analyze it regularly. 4. The NGA 911 Change Management system exceeds the requirements by adhering to our documented ITIL and FCAPS processes. NGA 911 has a Web-based portal to access and initiate the Change Management Process. NGA 911 will be available to authorized personnel including the State's program manager through the NGA 911 Web-Portal. All change requests will be entered into the IMS and assigned an Event ID. All coordination, communications, impacted stakeholders, and client approval will be logged on the Event ID. All Events in the IMS are stored and maintained for historical information for the term of the contract. The State and its representatives will have access to the data through the Web-Portal, however, NGA 911 will also provide copies of the data to the State on request and at the end of the contract. NGA 911 will provide monthly reports detailing change tickets opened, pending, resolved, and closed. NGA 911 will provide Change Management reports for system and other changes. These reports are also available to the State through the Web-Portal. NGA 911 incorporates the Information Technology Infrastructure Library (ITIL) version 3 service for problem and change management methods and procedures during the initial implementation and ongoing operations of the NGCS and ESInet. The NGA 911 documented Management Process includes a process to request change, completing Change Management forms detailing the description, reason and impact of change, activity, test plans, backout plans, and specific list of named systems, applications, and/or hardware to be affected by the change, and obtaining the Customer's approval. The Change Requests are discussed and approved in a Change Control Board Meeting. If the change involves other vendors, those vendors are included in the Change Control Board Meetings. NGA 911 has a process to communicate the requested change with the vendor. Approved changes are implemented and then the outcome of the change is presented at a subsequent Change Control Board Meeting. Routine changes such as system updates, patches, etc. are implemented according to customer maintenance windows and update and patch schedules.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 12	**NOC/SOC - Network Management System** **System and Network Management Software** Software packages are widely available for capturing, analyzing, and reporting the network's health based on the Simple Network Management Protocol (SNMP) traffic it receives. Provide the name and description of the management software that will be implemented including all functional modules associated with it (e.g., reporting, backup, and IP address management).	X			

Bidder Response:

NGA 911 uses NMIS and applied the design principles of A-CORD. The NGCS and networking elements are managed through an A-CORD based SDN Orchestration mechanism that is visualized through Grafana derived dashboards. An A-CORD compliant orchestration architecture combines the data coming from compute, storage, applications and networking elements to provide a unified view for security analytics, fault identification, performance analytics, policy configuration, addressing and provisioning. The three major components of our Network Management Information System are the Analytics Engines, Monitoring, and the SDN controller (shown below as the CORD Orchestration Platform).



	The NGCS is realized in vNF's - virtual Network Functions in AWS Virtual Private Clouds (VPC) and the ESInet are the networking elements. The Network Management Information System provides · Fault Identification · Performance Management · Network Provisioning · Network Addressing · Maintaining QoS and Policies

Any additional documentation can be inserted here:

NOC/ SOC 13	**NOC/SOC - NMIS Interworking with Elements and Services** Provide a detailed explanation and associated drawings explaining how the proposed solution interworks with all of the various elements and services of the proposed systems and network elements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The management software is a web-based solution and easily accessible to each individual PSAP and the Commission. NGA 911 can set levels of access or roles based upon the level of access required for each individual. For example, each PSAP would be granted access to the local PSAP, if there is a regional PSAP or an individual responsible for a region then that individual would be granted access to each of the locations that would fall under the individuals preview. The Commission would be granted access to each PSAP. Access is granted on the basis of ICAM (Identity, Credential, and Access Management). ICAM provides enterprise-class services for managing digital identities, credentials, and access to systems and applications. These services include centralized identity lifecycle management, role management for access control, automated account and access provisioning and de-provisioning. Our ICAM system provides access only to properly credential and then certified agents. Prior to the establishment of the PCA, NGA 911 and the Commission will agree on an interim agent credentialing method. Access is based on multi-factor authentication and all attempts whether successful or not are logged and analyzed for anomalies.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 14	**NOC/SOC - NMIS - Network Event Logging** **System and Network Event Logging and Reporting** The network management system shall capture real-time and historical tracking of network and system events, as well as event resolution of the IP network and attached systems. This is for logging errors and statistical information related to the health of the network and attached systems. Events shall include, but are not limited to, hardware (power, processor, interface cards, ports), software (operating system errors, database errors, application errors and failures), network (Quality of Service (QoS), Mean Opinion Score (MOS), jitter, latency, and packet loss))). The events recorded in this section are not related to the event logging of 911 requests for service in as part of NGCS option B requirement NGCS 13 Event Logging. Describe how the solution meets or exceeds the above requirement.	X			
	Bidder Response: The NGA 911 network management system shall capture real-time and historical tracking of network and system events, as well as event resolution concerning the ESInet on a 24 x 7 x 365 basis. Logging includes errors and statistical information related to the health of the network. Retention of network performance logs will comply with Pennsylvania's Office of Administration General Records Retention and Disposition Schedule. The NGA 911 Administration Web Portal monitors the health of the network and the NGCS. It logs and stores historical statistics for network and system events along with the health of the network and event resolution. The NGA 911 Logging Service solution is fully compliant with the NENA Detailed Functional and Interface Standards for the NENA i3 Solution Section 5.13 and NENA-STA-010 section 5.2.2.8. The NGA 911 logging service is a device that manages logging information for all devices in the NG9-1-1 network. At a site level, router and switch metrics include: ● Site availability ● CPU usage ● Memory usage ● Device temperature				

	● Interface availability ● Interface usage At a site level, access point metrics include: ● Channel usage ● Noise ● Interference ● Interface usage ● The number of clients currently connected to access points at the site Additional NGA 911 reports include: · Ring-time statistics · Trunk and line utilization · NGCS element usage volumes · Call processing times between elements · Agent activity · Call transfers · Call conferences · End-to-end call flow analysis Realtime network utilization and monitoring reports are made available to members. Below is a sample:

Network and system events are tracked and the data is pulled through syslog and SNMP trap.

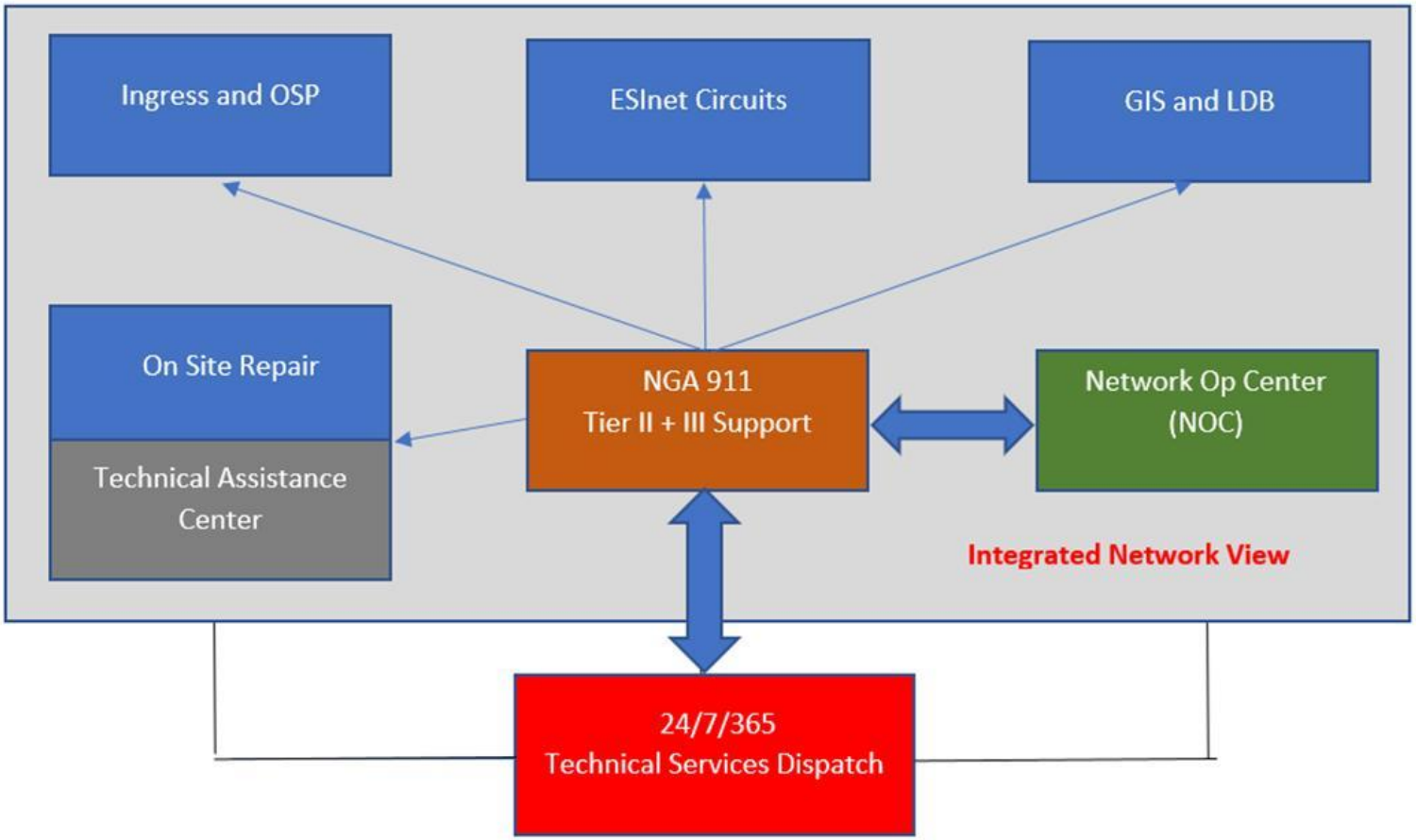
Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 15	**NOC/SOC - NMIS - Management System Interface to Incident Management System** This system should be part of, or interfaced with, the bidder's incident management system, or contain cross-reference abilities. Contractor shall maintain historical information for the term of the contract and provide copies of the data to the Commission on request, and at the end of the contract. Describe how the solution meets or exceeds the above requirement.	X			
	Bidder Response: NGA 911's Administrative Portal is a single Landing/Home Page for NGA 911 End Users, contractors and suppliers. The Administrative Web Portal allows the collaboration of all services and functional elements between all stakeholders. NGA 911's solution maintains all historical information for as long as defined by the customer. For the State of Pennsylvania, NGA 911 will maintain all historical information for the term of the contract and will provide copies of all data to the Commission at the end of the contract The NGA 911 Administrative Portal Interface is connected to the NGA 911 IMS and will be available to authorized personnel including the State's program manager through the NGA 911 Web-Portal. All network event logging is available via the NGA 911 Management Information System reporting module. All Events in the IMS are stored and maintained for historical information for the term of the contract. The State and its representatives will have access to the data through the Web-Portal, however, NGA 911 will also provide copies of the data to the State on request and at the end of the contract.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 16	**NOC/SOC - NMIS -Interfacing Between Solutions** Provide a detailed explanation and associated drawings explaining bidder's processes, tools, and procedures for interfacing with the bidder's monitoring solutions.	X			
	Bidder Response: NGA 911 has many years managing and integrating multi-vendor environments where they offer network management and operations services. Once the network final network design is approved by the State with NGA 911, NGA 911 will begin the eBonding process with the operations team in order to offer a single pane of glass and integrated trouble ticketing system. This approach provides the State with an overview of the network from a services perspective. NGA 911 manages the ESInet and NGCS through a number of suppliers. Inteliquent focuses on the Ingress Network and primarily the OSPs. It provides constant connections to the NMS for the LNG, LSRG, and the separate OSP channels. The ESInet circuits and interconnects are contracted through Nitel who brokers both Verizon and Comcast for the network. Fujitsu actively measures the performance of these suppliers with the Silver Peak monitoring system. Any violations of the underlying SLAs are immediately forwarded to the vendors with a parallel report going to NGA 911 for information and penalty purposes. Similarly, for GIS the basic services of the LDB, LVF, and ECRF are all monitored by Operations at the NOC. Alerts are sent to Datamaster with a notification to NGA 911 for trouble ticketing and customer support.				

Each contractor and supplier will have their own unique log on credentials. Each contractor and supplier associated with the ticket will receive email updates when a status change occurs in the Administrative Portal of the Integrated Network View.



Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 17	**NOC/SOC - Access to Technical Staff** 1. Detail the procedures by which bidder communicates with technical personnel from participating subcontractors, the Commission, and the participating PSAPs. 2. Specify the level of assistance required from such technical personnel to resolve service-related issues.	X			
	Bidder Response: 1. NGA 911 uses the NGA 911 Web-Portal's Communication Application, emails, and phone calls to communicate with our technical staff and suppliers. This platform for communication, work and information sharing allows for seamless communication when and where it is needed. NGA 911's robust social collaboration solution takes advantage of the ability to bring all stakeholders together to view conversations and engage in discussions thereby enabling problem solving and allowing for more informed decision making. NGA 911 will provide detailed explanation and graphical presentations showing how our solution meets or exceeds the above requirements. Communication Procedure:				

Step	Type	Description	Who
1	Open Communication Event	Open Communication Event. Provide a description of the issue and specify the level of assistance expected from technical personnel to resolve service-related issues.	Create a community of Stakeholders including Technical Personnel and other PSAP entities, NGA 911 Operations Support Manager and Project Manager.
2	Send Email	Send notification email of Communication Event Open.	To all identified Stakeholders
3	Event Logging	In order to maintain a complete historical record of all issues all relevant details must be maintained in the Communication Event	The Owner of the Event should ensure all records are accurate.
4	Event Investigation/Diagnosis	The Owner will determine the best method to resolution which may include involving other parties through one or more of the following: Email, in-person meeting, webinar, conference call	The Owner of the Event should identify the method of communication and initiate discussions.
5	Event Resolution	NGA 911 Technical Staff will resolve the event in collaboration with necessary parties.	All impacted Stakeholders
6	Event Closure	Event Owner will confirm that the event has been resolved and all impacted Stakeholders are satisfied and in agreement.	Event Owner

NGA 911 has a secure NGA 911 Web-Portal used to communicate with technical personnel from participating suppliers and the State entities. NGA 911 customers will receive 24x7x365 help desk and technical services support. NGA 911's intention is to be cognizant of time and engage the State's technical personnel only as needed, limiting the need for assistance from the State as we recognize

	they are busy. NGA 911 will engage with the State's technical personnel on a case by case basis. The State can obtain information, updates, and status of service issues, account information, including but not limited to help with the reporting system. The Commission and PSAP may request assistance or report trouble in three ways: • By dialing 1-877-899-8337; Option 2 and report trouble directly to the Help Desk or to ask for assistance on other non-emergency issues. • By sending an email to Support@NGA911.com • Web-Portal by accessing the Incident Management System (IMS) via the NGA 911 Dashboard 1. NGA 911 has qualified staff to resolve service-related issues. NGA 911 may require assistance in gaining access to our backroom equipment.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 18	**NOC/SOC - Notification** Specify how the bidder's NOC informs the Commission and the affected PSAPs or their designees of problems with the network, scheduled service and maintenance outages, and upgrades. Include all methods of notification used. Notifications for scheduled maintenance or outages shall be made no less than ten (10) business days in advance, except for emergency situations in which case, notification will be given immediately. Tickets related to the services delivered to subcontractors shall be forwarded automatically. Notification shall be provided via multiple communications means to the Commission and applicable PSAPs. Entities requiring notification may change, depending on the alarm or incident. Provide a detailed explanation explaining how the solution meets or exceeds the above requirements, including the methods of communications used.	X			
	Bidder Response: For Network scheduled outages and upgrades the NGA 911 Operations Staff will send an email notification to the Commission's and PSAP designee concerning scheduled release installations, planned upgrades, and network outages that may impact Commission or PSAP. NGA 911 will require acknowledgement of notification. Our Service Management Center within our Network Operations Center (NOC) monitors the State's network 24x7x365 to ensure impairments are rapidly addressed. Expert Monitoring systems give an intuitive view so that personnel can react quickly even to hints of impairment. The Commission and PSAP will be able to set up, manage, and change their profile indicating their personnel to be notified and by which means based upon the PSAP's profile, alarm type or incident. The IMS generates an incident that remains open and in queue until it is resolved. Once the Commission or PSAP notifies NGA 911 of an issue, they will be provided a unique incident number, date and time opened, status of the ticket, and description of the problem reported via email, if available, or by voice. All notes regarding troubleshooting and/or research performed are documented in the notes field and are readily available to the customer. Each incident is assigned a priority level and updates or changes to the priority level are automatically entered in the tracking log with the user ID of the individual making the change along with a timestamp. Additionally, the NGA 911 Trouble Ticketing System allows the customer to pull their reports of open and closed incidents. NGA 911's IMS automatically sends email updates to members whenever a change is made to the incident including all notes made to the tracking log, priority level changes, and incident closure. Additionally, a Technical Service Representative will be assigned to monitor, and notification the member via telephone with updates. Below is the escalation matrix helps ensure that available resources are focused on problems that severely affect service. This table defines when additional resources are notified to ensure management is aware of problems and can troubleshooting support. See the following table:				

Rank and SLA	Level 1 Critical	Level 2 Major	Level 3 Minor	Level 4 Standard
Response/ Acknowledge	< 15 minutes	< 30 minutes	8 hours	Based on request
Tech on Site (if required)	0-2 hours	2 hours	Next Business Day	Based on request
Escalation Threshold	1 hour	2 hours	48 hours	As needed
Communication Objective	Hourly	Every 2 hours	Daily	As needed

The Commission and PSAP may request assistance or report trouble in three ways:

- By dialing 1-877-899-8337; Option 2 and report trouble directly to the Help Desk
- By sending an email to Support@NGA911.com
- Via Web-Portal by accessing the Incident Management System (IMS) via the NGA 911 Dashboard

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 19	**NOC/SOC - Executive Dashboard** Contractor shall provide a web-based executive dashboard or similar tool, providing near real-time visibility of network status displayed geographically with service impact levels color-coded. Open ticket status shall be available to users through this dashboard. Describe how the solution meets or exceeds the above requirement.	X			

Bidder Response:

The NGA 911 solution has a web-based comprehensive dashboard tool that provides near real-time visibility for:

Escalation Status - the NGA 911 Dashboard Trouble Reporting Tool has three different automatic escalation types. These three types of escalations are built into NGA 911's Intelligent Business Rules (IBR) process that are based on predefined trouble ticket criticality. These rules can be updated to meet the Nebraska automated escalation business rules.

- Priority Based Escalation - Automatically assigns staff based on priority of ticket. Low priority tickets are handled by Technical Support staff while high priority tickets automatically escalate to management for review and support.
- Complexity Based Escalation - Engineering levels are created in the IBR that identifies more complex tickets and automatically escalates to the more Senior Engineers.
- Service Level Agreement (SLA) Based Escalation - SLAs are built into the IBR that will automatically escalate trouble tickets based on the SLA. The IBR will also proactively assign a ticket to Senior Engineers with a notification to Senior Management when a ticket is approaching a breach of contract.

The Dashboard and its associated transparency are vital to project success for all stakeholders during both test and live because issues must be identified immediately and handled transparency so that a strong knowledge base can be created to operate this new NG9-1-1 solution for the state.

Available Real Time for Print, PDF, or CSV: The statistical data in different categories can also be printed or exported to a CSV file for additional data analysis. PDF reports can also be generated.

The top-level categories displayable dashboards on the top-level screen consist of the following:

Ingress/Egress Bandwidth Utilization by Application: This enables you to see the amount of bandwidth each application uses as it ingresses and egresses the SD-WAN, which is useful for underlay WAN capacity planning over time. It is also useful to identify different applications in use for which you may want to set up additional QoS or Security policies.

Health Map of all SD-WAN sites: This gives you a high-level view of the overall health of all of the sites in a single graph. The health is color-coded green (normal operation)/yellow (minor issues)/red (major issues). You can select to see the site health for all Alarms,

QoS (latency, loss, jitter), and MOS (mean opinion score for voice quality) and sort the health for each site in hourly, daily or weekly views.

Ingress/Egress Loss / Jitter / Latency for each site (displayed as 3 separate categories): This gives you a view (in % or ms) of the QoS performance (Loss/Jitter/Latency) in each direction for each Tunnel overlay between SD-WAN Edge pairs and the underlay WAN circuits at each site.

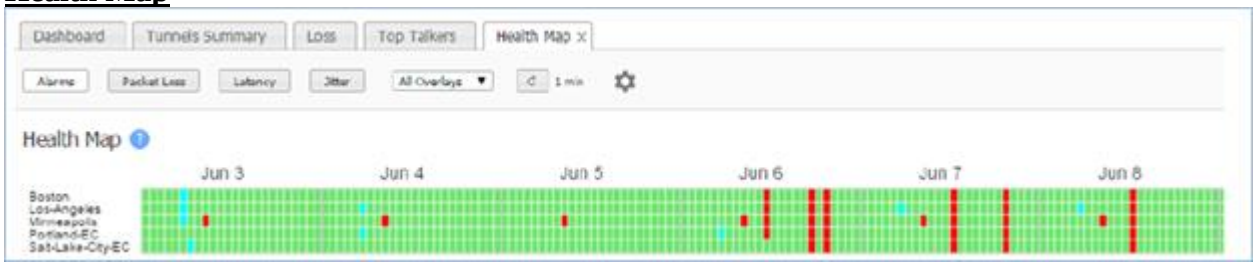
Top Talkers: This gives you a list of trunks and media paths listed in order of ingress/egress bandwidth usage. It enables you to identify different applications in use for which you may want to set up additional QoS or Security policies.

Overlay Ingress/Egress Bandwidth: This gives you a list of each SD-WAN overlay and the amount of bandwidth each uses

Ingress/Egress Overlay/Underlay Bandwidth: This gives you a multi-layer view of the SD-WAN overlay and underlay WAN bandwidth for both ingress and egress bandwidth. This enables you to see the overall SD-WAN bandwidth in conjunction with the bandwidth for each underlay WAN over which the SD-WAN operates at a site.

Network Topology: This gives you a network topology of all locations interconnected on the SD-WAN overlaid onto a geographic map which you can zoom in/out. This enables you to see the health of the entire SD-WAN including all SD-WAN Edges, and SD-WAN overlays & underlay WANs between SD-WAN Edges (sites) using the color-coding green (normal operation)/yellow (minor issues)/red (major issues).

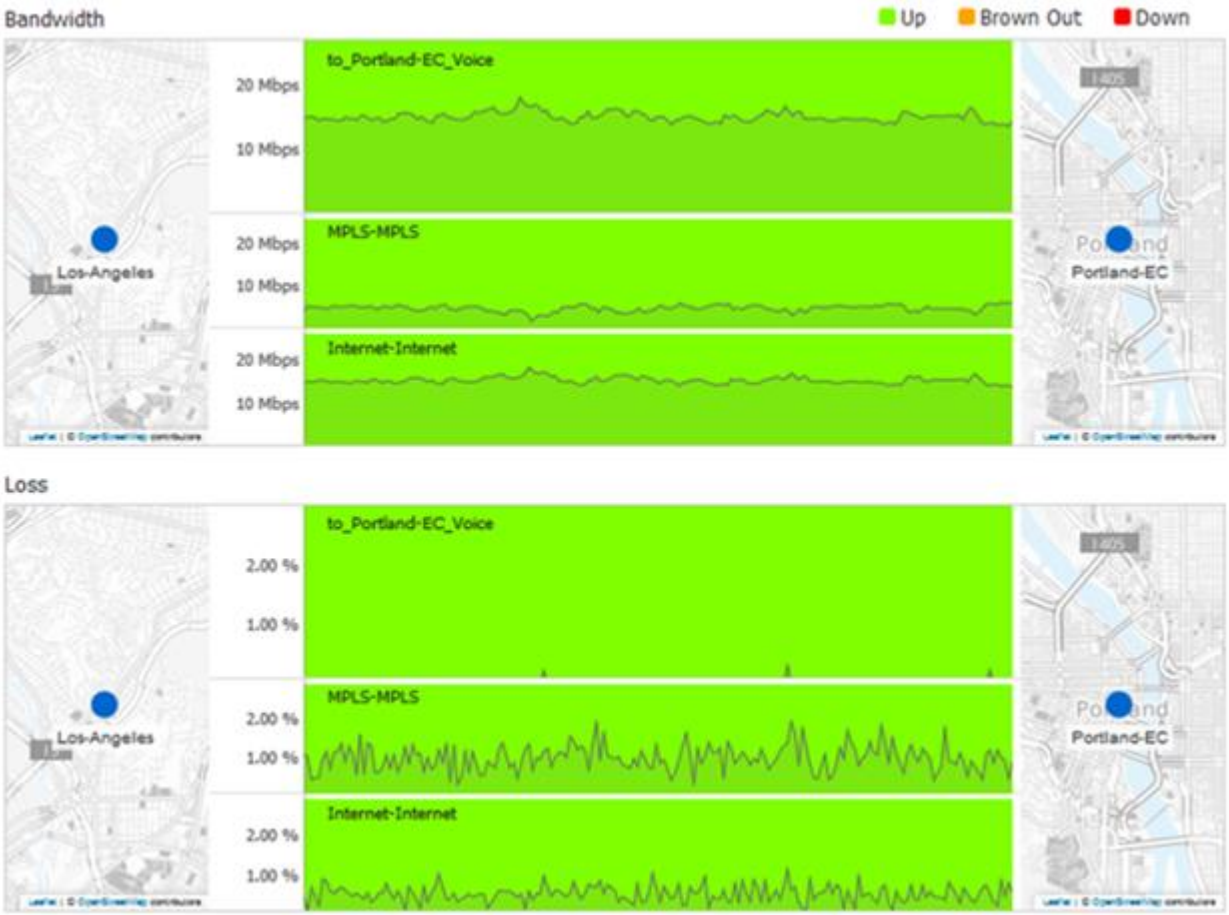
Health Map



Bandwidth

Live View
Bandwidth
Loss
Jitter
Latency
Charts
Traceroute
Lock Scale
Bandwidth
Up
Brown Out
Down
to_brodio-ecvc_RealTime
4.0 Mbps
2.0 Mbps
MPLS-MPLS
4.0 Mbps
2.0 Mbps
Internet-Internet
4.0 Mbps
2.0 Mbps
brodio-ecvd
brodio-ecvc
Map Data
Terms of Use
Map Data
Terms of Use

Latency



Network and system events are tracked and the data is pulled through syslog and SNMP trap.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 20	**NOC/SOC - Escalation Procedures** 1. Outline a detailed regional-level escalation process to be used during incidents that affect service, particularly those that result in critical service outages. 2. Describe how discrepancies in the perception of service level agreement (SLA) incident levels may be escalated and addressed. These procedures shall be maintained and accessible via an online portal. This escalation notification process shall be integrated with the notification processes described above, based on the problem reported.	X			

Bidder Response:

1. The table below describes the automatic notification and escalation process based on trouble severity level. Each PSAP/State, jurisdiction-level, has the ability to request escalation outside the automated process. NGA 911's NOC will notify the adjacent jurisdictions if they have that presence set in the NGA 911 web-based portal.

   In addition, NGA 911 will electronically report outages to the FCC's Network Outage Reporting System (NORS) within 120 minutes of discovering an outage lasting at least 30 minutes that potentially affects a PSAP or at least 900,000 "user minutes," which are calculated by multiplying the outage's duration by the number of potentially impacted end users.

2. For discrepancies in the perception of SLA incident level assigned to a trouble event a PSAP/State can call the Director of Services to request the ticket be reclassified to the correct severity level and appropriate response times.

   The Commission and PSAP may request assistance or report trouble in three ways:

   - By dialing 1-877-899-8337; Option 2 and ask for the trouble event to be reclassified directly to the Help Desk
   - By sending an email to Support@NGA911.com asking for the trouble event to be reclassified
   - Via Web-Portal by accessing the Incident Management System (IMS) via the NGA 911 Dashboard update the trouble ticket asking the trouble event to be reclassified

See below:

Any additional documentation can be inserted here:

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

Elapsed Time	Critical Severity Level 1	Major Severity Level 2	Minor Severity Level 3	Informational Severity Level 4
30 minutes	**Escalation Level:** NOC notified, Director of Services, Chief Technology Officer, and Chief Executive Officer 1) Trouble ticket opened and sent by email 2) Text sent 3) Voice notification			
30 minutes		**Escalation Level:** NOC notified 1) Trouble ticket opened and sent by email 2) Text sent		

		3) Voice notification		
1 hour	Escalation Level: All Executive Management		Escalation Level: NOC notified Trouble ticket opened and sent by email	
2 hours		Escalation Level: Director of Services 1) Trouble ticket updated and sent by email 2) Text sent 3) Voice notification		Escalation Level: NOC notified Trouble ticket opened and sent by email

4 hours	**Escalation Level:** **All Executive Management** **1) Trouble ticket updated and sent by email** **2) Text sent** **3) Voice notification**			
8 Hours		**Escalation Level:** **Sr VP Operations and Chief Technology Officer** **1) Trouble ticket updated and sent by email** **2) Text sent** **3) Voice notification**		

24 hours		**Escalation Level:** **Sr VP Operations, Chief Technology Officer, and Chief Executive Officer** **1) Trouble ticket updated and sent by email** **2) Text sent** **3) Voice notification**	**Escalation Level:** **Director of Services** **Updates to trouble ticket by email**	
7 days			**Escalation Level:** **Sr VP Operations** **Updates to trouble ticket by email**	
Weekly				**Escalation Level:** **Director of Services** **Updates to trouble ticket by email**

30 Calendar Days				**Escalation Level:** **Sr VP Operations** **Updates to trouble ticket by email**

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 21	**NOC/SOC -Statement on Standards for Attestation Engagement Number 16** Bidder shall demonstrate compliance with the Statement on Standards for Attestation Engagements Number 16 (SSAE 16). The applicable report from an SSAE 16 engagement is the Service Organization Controls 1 (SOC 1) report. 1. If bidder is proposing services, provide a detailed explanation of how bidder has complied with SSAE 16 for similar solutions, and how this would be implemented with the Commission's NG911 implementation. 2. Provide with the detailed explanation and graphical representation explaining how the solution meets or exceeds the above requirement	X			

Bidder Response:

NGA 911 complies with the Statement on Standards for Attestation Engagements (SSAE) No. 16. by coordinating with the Commission regarding the incorporating of our standard QMS with a process and standard specific to the State of Nebraska.

NGA 911 will work with the Commission to implement the proper controls to comply with the Commission's own SOC 1 criteria. The NGCS is implemented on a platform that has been validated and found compliant with the following controls.

Control Objective	**Control Objective Description**
C01	Controls provide reasonable assurance that information security policies have been implemented and communicated throughout the organization.
C02	Controls provide reasonable assurance that procedures have been established so that employee user accounts are added, modified and deleted in a timely manner and reviewed on a periodic basis.

	C03	Controls provide reasonable assurance that policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.	
	C04	Controls provide reasonable assurance that data handling between the customer's point of initiation to a vendor storage location is secured and mapped accurately.	
	C05	Controls provide reasonable assurance that physical access to data centers is restricted to authorized personnel and that mechanisms are in place to minimize the effect of a malfunction or physical disaster to data center facilities.	
	C06	Controls provide reasonable assurance that changes (including emergency/non-routine and configuration) to existing IT resources are logged, authorized, tested, approved and documented.	
	C07	Controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing.	
	C08	Controls provide reasonable assurance that system incidents are recorded, analyzed and resolved.	

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NOC/ SOC 22	**NOC / SOC - Configuration Backup and Restoration** 1. The bidder shall deploy and provide detailed descriptions of bidder and any subcontractors' capabilities to automatically or routinely back up configuration data and define the conditions under which the configuration of network elements, such as routers or switches, will be restored, and the process that will be used. A reporting process shall confirm regularly scheduled (e.g., monthly, quarterly) backup and restoration, and provide sufficient details on backup and restoration activity. 2. Describe the bidder's abilities to perform on-demand backups, such as at the end of a successful configuration change. A reporting process shall confirm on-demand backup and restoration and provide sufficient details on backup and restoration activity. 3. Describe bidder's COOP as it applies to the NGCS and delivery of 911 traffic via IP network to the respective host locations. 4. Provide a detailed explanation and any associated drawings explaining how the proposed processes and procedures provide the ability to manage these configuration backup and restoration processes in a manner that has no negative impact on the total Commission ESInet and NGCS solution.	X			

Bidder Response:

1. The NGA 911 robust and reliable data backup system routinely performs daily and on-demand back-up and restoration of data used for all NGCS components in its system. The NGA 911 data back-up system will do the following:

   NGA 911 performs automatic daily backup of our data and systems

   NGA 911 maintains minimum ninety (90) calendar days of data backups

- Archive and securely transport to a secure external site at least two weekly copies of the data and systems backups
- Provide daily backup reports of all successful/failed system backups/archives to the State
- Provide data recovery services that will be accomplished without impact to system function
- Will provide a copy of all data to the State upon request

<u>NGA 911 procedures to perform automated, regularly scheduled, and on-demand backups:</u>

NGA 911 regularly and routinely back's up configuration data and performs software upgrades in accordance with our DevOps Process. Previous working configurations can be invoked and loaded in parallel with the current release to test side-by-side performance on active-active systems. New functions and features are subject to thorough and robust testing in a pre-production

environment. When code is ready for deployment the release process is structured to maintain the current load for a fixed period of time. Releases are made only on one copy of redundant deployments. The operational performance of new releases are continuously monitored to verify conformance with specifications. Any general release is completed when specifications are verified over a defined period. In an active-active environment, the performance of the new load is directly compared to the current load. In the case of an Operational Exception Fault (during Test Release and Full Release); Restoration or Fallback to previous version is automated so that both active-active instances are returned to the current stable release.

2. NGA 911 constantly performs on-demand back-ups at the end of every successful configuration change and logs the change with complete details on backup and restoration activity.

3. Documented Continuity of Operations Plan (COOP)
The NGA 911 Continuity of Operations Plan (COOP) or Disaster Recovery Plan outlines problem change management systems, reporting systems, escalation plan, and conformance with best practices for service delivery management is described below.

NGA 911 has a recovery plan if all of these measures fail. From that perspective our plan involves a well architected response framework. If due to circuit cuts then the TSP is notified and implemented by the NOC with direct communications to the service provider, the FCC, and of course to the State. If in fact all networks and data centers and redundant systems are down, we have the capability of bringing up new containers on other networks and cloud providers such as GCP and Azure. Restoration (if ever necessary) in the cloud is typified by the following Recovery Time Objects (RTO):

• Containers – failover happens over the course of seconds or virtually instantaneously
• High Availability solutions – failover happens over the course of seconds / minutes
• Tape / Image – manual restoration occurs over the course of hours/days (note: all of NGA 911 Core Services and FE's are in Containers and H/A configurations and the Tape/Image restoration is not applicable to basic call handling scenarios and only to archived data sets not immediately needed for the operation of the NGCS)

Additionally, we will integrate our recourse/response plans with the Commission, PSAP and State NIMS and ICS protocols. Escalation procedures trigger notifications to operations and County, regional, state and Federal authorities of incidents and appropriate remedies for restoration. Escalation is also used if the "Investigation and Diagnosis" and "Resolution and Recovery" are not resolved in a timely manner, notifying senior management to take necessary action to resolve any issues. Hierarchic escalation consists of two parts, one related to the technical efforts to restore the service (led by incident manager or a first-level operations technician and managed through a technical bridge), and the other related to NGA 911's communication management. There are different escalation paths for critical and non-critical incidents. For critical incidents, the appropriate managers from operations or from the State must be notified. Procedures are aligned to the National Incident Management System (NIMS) to facilitate coordination with public safety entities. These processes cover release management, business continuity, disaster recovery management, change management process, capacity management, national and local

	support structure for network configuration, maintenance and monitoring, protocols, and deployable assets for natural disasters. NGA 911 recommends that the Disaster Recovery plan be tested with the PSAP on a quarterly basis to ensure that all functions work as designed. If there are any changes due to a Memorandum of Understanding (MOU) or an agreement between two or more PSAPs, the PSAPs can schedule a test with NGA 911 to verify that new routes are functioning properly or as designed. 4. NGA 911 regularly and routinely back's up configuration data and performs software upgrades in accordance with our DevOps Process. Previous working configurations can be invoked and loaded in parallel with the current release to test side-by-side performance on active-active systems. New functions and features are subject to thorough and robust testing in a pre-production environment. When code is ready for deployment the release process is structured to maintain the current load for a fixed period of time. Releases are made only on one copy of redundant deployments. The operational performance of new releases is continuously monitored to verify conformance with specifications. Any general release is completed when specifications are verified over a defined period. In an active-active environment, the performance of the new load is directly compared to the current load. In the case of an Operational Exception Fault (during Test Release and Full Release); Restoration or Fallback to previous version is automated so that both active-active instances are returned to the current stable release.				

Any additional documentation can be inserted here:

NOC/ SOC 23	**NOC/SOC – Third-Party Management** The Commission is seeking the optimum value provided by best-of-class products and services integrated as part of the total IP network solution. This may present a situation where no single manufacturer or supplier can provide a public safety-grade, unified NOC/SOC accountable for all components, products, and services that comprise the Commission's total IP network solution. Consequently, the Commission may find it beneficial to have a third party provide that overarching NOC/SOC service. A third-party NOC/SOC provider may be responsible for functioning as an umbrella for monitoring all of the Contractor's products and services, including collaboration with the Contractor's NOC/SOC. To facilitate that capability, the third-party NOC/SOC shall have a view into all elements that are under SLAs. Bidder's NOC/SOC NMIS and/or incident-tracking tools shall have the ability to perform eBonding, which enables bidirectional data synchronization. 2. Provide a detailed narrative discussing bidders experience in providing access to third-party NOC/SOC, overarching support as well as for each of the requirements in Third-Party NOC/SOC Support below.	X			

In support of the Commission's consideration of such an option, bidder shall indicate the compliance level of bidder's experience in providing access to third-party NOC/SOC overarching support, as related to the requirements identified in the table below.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
Change management processes	X			
Coordinating and managing trouble tickets to resolution from bidder and multiple suppliers.	X			
Trouble ticket report management (reports may be daily, weekly, monthly, quarterly, or yearly).	X			
Notification processes for bidder and suppliers, and any other entities or people designated by the Commission.	X			
System alarm access in the form of SNMP or syslog data.	X			
Experience and processes for interworking of multiple public safety data system suppliers.	X			

Bidder's Detailed Response:

The NGA 911 solution has a NOC/SOC. All components of the NGA 911 solution are monitored 24x7x365 by our NOC/SOC. The NGA 911 NOC/SOC comply and meet the following requirements.

- Change management processes.
- Coordinating and managing trouble tickets to resolution from the Offeror of record and its sub Offerors.
- Trouble ticket report management.
- Notification processes for the Offeror of record and its sub Offerors, and any other entities or people designated by the Commission.
- System alarm access in the form of simple network management protocol (SNMP) or syslog data.
- Experience and processes for interworking of multiple public safety data system suppliers.

Third Party NOC/SOC Support

Requirement	Complies	Complies Partially	Complies with Future Capabilities	Does Not Comply

4.9.13.1 Change management processes	**X**			
4.9.13.2 Coordinating and managing trouble tickets to resolution from contractor and multiple suppliers	**X**			
4.9.13.3 Trouble ticket report management (reports may be daily, weekly, monthly, quarterly, or yearly)	**X**			
4.9.13.4 Notification processes for contractor and suppliers and any other entities or people designated by the Commission	**X**			
4.9.13.5 System alarm access in the form of SNMP or syslog data	**X**			
4.9.13.6 Experience and processes for interworking of multiple public safety voice and data system suppliers	**X**			

Additionally, NGA 911 NOC/SOC offers fully managed service. These administrative and support services include:

- 24x7x365 Help Desk with NOC services

- 24x7x365 SOC services
- 24x7x365 Software support
- 24x7x365 Network monitoring and Security
- 24x7x365 Administrative Support
- Training
- Management Information Services
- Assessment and Studies
- 24x7x365 Technical Support
- 24x7x365 Maintenance

The above services are provided in connection with Fujitsu which operates NGA 911's NOC/SOC at Tier I and is E-bonded into our Tier II and Tier III support teams.

Any additional documentation can be inserted here:
Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 1	**General Operations - Service Level Agreements** **System Capacities and Performance** 1. Provide capacity levels of each element of the IP Network This may be in terms of busy-hour calls, network bandwidth, or any other applicable measure. The proposed solution shall be capable of handling current and planned IP traffic and usage plus 50 percent capacity growth over the term of the contract. 2. Specify lead times required to increase capacities on each element of the IP network.	X			

Bidder Response:

1. The NGA 911 solution is designed with a minimum level of bandwidth to support the delivery of calls and associated data from originating service providers or other integrated ESInets to the PSAPs. The NGA 911 solution has a minimum recommended IP access of an Ethernet Circuit of 10 Mbps for PSAPs that primarily receive voice and text services. Any circuits provisioned as part of this project will be capable and software upgradeable to support significantly higher data rates when required. For example, in the future, when a PSAP desires to receive video, additional circuit bandwidth will be simply acquired.

   The bandwidth required is determined by the size, position number, and traffic loading offered and calculated appropriately. We make bandwidth calculations based on the Erlang C formula and find that at a minimum recommended bandwidth of 10 Mbs per PSAP we offer a very large buffer for traffic today and to allow for well above 50 percent traffic usage growth in the future. Regardless, bandwidth at the PSAP is easily expanded if traffic or new applications demand it.

   On the network side, the NGCS and all Functional and Network Elements are designed using Elastic Load Balancing and Auto Scaling. As such, NGA 911 commits to offering the following increases in Capacity/Load without any additional charges over the life of the contract:

Function/Criteria	**Increase**
BCF	300%
NGCS	500%
Connections	300%

	2. Through a self-service portal for most of the bandwidth on the system, provisioning is immediate. There is essentially no lead time required to increase capacity on the circuits up to 100Mbps for most circuits and 1Gbps on some. 3. Failure to meet the SLA objective for one month shall result in a 10% credit/or adjustment of the Total Monthly Recurring Cost (TMRC) of the circuits that do not offer 50% capacity over the busy hour traffic under contract for that month. Next consecutive month fails to meet the SLA objective shall result in a 20% credit/or adjustment of the TMRC of the circuits that do not offer 50% capacity over the busy hour traffic under contract for that month. Each additional consecutive month fails to meet the SLA objective shall result in a 50% credit/or adjustment of the TMRC of the circuits that do not offer 50% capacity over the busy hour traffic under contract for that month. NGA 911 uses a combination of NMS, MIS, logs, SNMP traps and algorithms to collect, collate, analyze and report on KPIs through our Web-based Portal.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 2	**Service Level Agreements - System Performance** **Network Latency** Specify the guaranteed maximum latency across the backbone network under a full-load condition, and include how that information will be gathered, calculated and provided to the Commission and the affected PSAPs.	X			

Bidder Response:

NGA 911 addresses the Packet Latency NENA standard by using dedicated circuits to ensure fewer network hops to provide low latency performance. Media and data traffic are backhauled on the private Amazon Web Service (AWS) Network and over a multi-supplier bonded, aggregated, performance optimized SD-WAN to and from the PSAP to guarantee a maximum latency of 30ms across the network.

The latency is calculated through the SD-WAN technology that is deployed end-to-end by NGA 911 and is Network Monitored by the NGA 911 NOC. The NOC appends flow tracing packets to each and every packet traversing the whole ESInet from ingress to egress whether signaling or media. These "sidecars" are used to measure latency, jitter, route, and travel times for each and every route and interconnect service provider on the net. The NGA 911 SDWAN also accommodates and corrects for any loss characteristics associated with the underlying carrier's network or any applicable wireless link we use to provide the ESInet to the state.

Failure to meet the SLA objective for one month shall result in a 10% credit/or adjustment of the Total Monthly Recurring Cost (TMRC) of the circuits that exceed the maximum latency over the busy hour traffic under contract for that month.

Next consecutive month fails to meet the SLA objective shall result in a 20% credit/or adjustment of the TMRC of the circuits that exceed the maximum latency over the busy hour traffic under contract for that month.

Each additional consecutive month fails to meet the SLA objective shall result in a 20% credit/or adjustment of the TMRC of the circuits that exceed the maximum latency capacity over the busy hour traffic under contract for that month.

NGA 911 uses a combination of NMS, MIS, logs, SNMP traps and algorithms to collect, collate, analyze and report on KPIs through our Web-based Portal.

System and Network event logging are part of the NMIS and statistics and data related to events such as processor, ports, software (operating system errors, database errors, application errors and failures), network (quality of service [QoS], mean opinion score [MOS], jitter, latency, and packet loss) are measured, logged, analyzed and available for viewing on the Executive Dashboard and OSS interfaces.

	Reports are available on a daily, weekly, monthly, quarterly, annual, and custom basis and accessed from the NGA 911 Reports Engine.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 3	**Service Level Agreements - System Performance** **Point of Presence (POP) to POP** Specify the guaranteed maximum latency from interconnection facility to interconnection facility, and include how that information will be gathered, calculated and provided to the Commission and the affected PSAPs.	X			
	Bidder Response: The guaranteed maximum latency from interconnection facility to interconnection (IXC) facility shall not exceed 30 ms. The information will be gathered by the NMS utilizing both periodic ping tests and NetFlow sidecar analysis. The collected data from both will be used to calculate the maximum sustained latency (a network convergence that occurs at .001% of the time and does not exceed 54 ms – will be judged in compliance) of 30 ms for the reporting period (monthly). Failure to meet the SLA objective for one month shall result in a 10% credit/or adjustment of the Total Monthly Recurring Cost (TMRC) of the IXC to IXC circuits that exceed the maximum latency over the busy hour traffic under contract for that month. Next consecutive month fails to meet the SLA objective shall result in a 20% credit/or adjustment of the TMRC of the IXC to IXC circuits that exceed the maximum latency over the busy hour traffic under contract for that month. Each additional consecutive month fails to meet the SLA objective shall result in a 50% credit/or adjustment of the TMRC of the IXC to IXC circuits that exceed the maximum latency capacity over the busy hour traffic under contract for that month. NGA 911 uses a combination of NMS, MIS, logs, SNMP traps and algorithms to collect, collate, analyze and report on KPIs through our Web-based Portal. System and Network event logging are part of the NMIS and statistics and data related to events such as processor, ports, software (operating system errors, database errors, application errors and failures), network (quality of service [QoS], mean opinion score [MOS], jitter, latency, and packet loss) are measured, logged, analyzed and available for viewing on the Executive Dashboard and OSS interfaces. Reports are available on a daily, weekly, monthly, quarterly, annual, and custom basis and accessed from the NGA 911 Reports Engine.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 4	**Service Level Agreements - System Performance** **POP to Endpoints** Specify the guaranteed maximum latency from interconnection facilities to the network interface device located at the entrance to the hosts' premises, and include how that information will be gathered, calculated and provided to the Commission and the affected PSAPs.	X			
	Bidder Response: The guaranteed maximum latency from interconnection facilities to the network interface device located at the entrance to the hosts' premises shall not exceed 30 ms. The information will be gathered by the SD-WAN utilizing provided side car analysis. The collected data from both will be used to calculate the maximum sustained latency (a network convergence that occurs at .001% of the time and does not exceed 54 ms – will be judged in compliance) of 30 ms for the reporting period (monthly). Failure to meet the SLA objective for one month shall result in a 10% credit/or adjustment of the Total Monthly Recurring Cost (TMRC) of the IXC to Host circuits that exceed the maximum latency over the busy hour traffic under contract for that month. Next consecutive month failure to meet the SLA objective shall result in a 20% credit/or adjustment of the TMRC of the IXC to Host circuits that exceed the maximum latency over the busy hour traffic under contract for that month. Each additional consecutive month failure to meet the SLA objective shall result in a 50% credit/or adjustment of the TMRC of the IXC to Host circuits that exceed the maximum latency capacity over the busy hour traffic under contract for that month. NGA 911 uses a combination of NMS, MIS, logs, SNMP traps and algorithms to collect, collate, analyze and report on KPIs through our Web-based Portal. System and Network event logging are part of the NMIS and statistics and data related to events such as processor, ports, software (operating system errors, database errors, application errors and failures), network (quality of service [QoS], mean opinion score [MOS], jitter, latency, and packet loss) are measured, logged, analyzed and available for viewing on the Executive Dashboard and OSS interfaces. Reports are available on a daily, weekly, monthly, quarterly, annual, and custom basis and accessed from the NGA 911 Reports Engine.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 5	**Service Level Agreements - System Performance** **Mean Opinion Score (MOS)** Bidder shall guarantee, in the response, a consistent MOS of 4.0 or better across all network links transporting media streams from interconnection facilities to the network interface device located at the entrance to the hosts' premises, and include how that information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: NGA 911 guarantees a consistent MOS of 4.0 or better across all network links transporting media streams from interconnection facilities to the network interface device located at the entrance to the hosts' premises. The information will be gathered by the NMS and SD-WAN utilizing the injection of known media into the RTP path – that transmit speech over a network and compare that speech to how it arrives on the other end analysis. The collected data from both will be used to calculate the average and minimum MOS of 4.0 or better for the reporting period (monthly). The average MOS will be reported to the Commission as a KPI on the monthly report. Failure to meet the SLA objective for one month shall result in a 10% credit/or adjustment of the Total Monthly Recurring Cost (TMRC) of the circuits that do not meet the MOS of 4.0 or better under contract for that month. Next consecutive month failure to meet the SLA objective shall result in a 20% credit/or adjustment of the TMRC of the circuits that do not meet the MOS of 4.0 or better under contract for that month. Each additional consecutive month failure to meet the SLA objective shall result in a 50% credit/or adjustment of the TMRC of the circuits that do not meet the MOS of 4.0 or better under contract for that month. System and Network event logging are part of the NMIS and statistics and data related to events such as processor, ports, software (operating system errors, database errors, application errors and failures), network (quality of service [QoS], mean opinion score [MOS], jitter, latency, and packet loss) are measured, logged, analyzed and available for viewing on the Executive Dashboard and OSS interfaces. Reports are available on a daily, weekly, monthly, quarterly, annual, and custom basis and accessed from the NGA 911 Reports Engine.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 6	**Service Level Agreements - System Performance** **Packet Loss** Specify the guaranteed maximum end-to-end packet loss across the network. This specification also shall include any loss characteristics associated with another carrier's network or any applicable wireless links, including how that information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested.	X			
	Bidder Response: NGA 911 addresses the Packet Loss NENA standard by designing a solution to minimize end-to-end packet loss across the NGA 911 ESInet. NGA 911 anticipates and guarantees an end-to-end packet loss budget of 0.015 (1.5%). NGA 911 NMS can account for and mitigate networks over which NGA 911 transports data (packets) over regardless of medium (fiber, cable, wireless, microwave, etc.). Packet loss is calculated as the total packets lost vs the total sent and is derived from TCP congestion and for media by FEC – forward error control algorithms inherent in our media delivery solution. Failure to meet the SLA objective for one month shall result in a 10% credit/or adjustment of the Total Monthly Recurring Cost (TMRC) of the circuits that exceed the packet loss budget under contract for that month. Next consecutive month failure to meet the SLA objective shall result in a 20% credit/or adjustment of the TMRC of the circuits that exceed the packet loss budget under contract for that month. Each additional consecutive month failure to meet the SLA objective shall result in a 50% credit/or adjustment of the TMRC of the circuits that exceed the packet loss budget under contract for that month. NGA 911 uses a combination of NMS, MIS, logs, SNMP traps and algorithms to collect, collate, analyze and report on KPIs through our Web-based Portal. System and Network event logging are part of the NMIS and statistics and data related to events such as processor, ports, software (operating system errors, database errors, application errors and failures), network (quality of service [QoS], mean opinion score [MOS], jitter, latency, and packet loss) are measured, logged, analyzed and available for viewing on the Executive Dashboard and OSS interfaces. Reports are available on a daily, weekly, monthly, quarterly, annual, and custom basis and accessed from the NGA 911 Reports Engine.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 7	**Service Level Agreements - System Performance** **Network Latency** Specify the guaranteed maximum end-to-end network latency across the network. This specification also shall include any latency associated with another carrier's network or any applicable wireless links, including how that information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested.	X			
	Bidder Response: The guaranteed maximum end-to-end network latency across the network shall not exceed 50 ms. The information will be gathered by the NMS, SD-WAN, and Ingress and Egress BCFs utilizing Netflow and additional side car analysis. The collected data from all three will be used to calculate the maximum sustained latency (a network convergence that occurs at .001% of the time and does not exceed 54 ms – will be judged in compliance) of 50 ms for the reporting period (monthly). The maximum end-to-end latency will be reported to the Commission as a KPI on the monthly report. Failure to meet the SLA objective for one month shall result in a 10% credit/or adjustment of the Total Monthly Recurring Cost (TMRC) of the circuits that exceed the maximum end-to-end latency over the busy hour traffic under contract for that month. Next consecutive month failure to meet the SLA objective shall result in a 20% credit/or adjustment of the TMRC of the circuits that exceed the maximum end-to-end latency over the busy hour traffic under contract for that month. Each additional consecutive month failure to meet the SLA objective shall result in a 50% credit/or adjustment of the TMRC of the circuits that exceed the maximum end-to-end latency over the busy our traffic under contract for that month. System and Network event logging are part of the NMIS and statistics and data related to events such as processor, ports, software (operating system errors, database errors, application errors and failures), network (quality of service [QoS], mean opinion score [MOS], jitter, latency, and packet loss) are measured, logged, analyzed and available for viewing on the Executive Dashboard and OSS interfaces. Reports are available on a daily, weekly, monthly, quarterly, annual, and custom basis and accessed from the NGA 911 Reports Engine.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 8	**Service Level Agreements - System Performance** **Jitter** Specify the guaranteed maximum end-to-end jitter across the network. This specification also shall include any jitter characteristics associated with another carrier's network or any applicable wireless links, including how that information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested.	X			
	Bidder Response: NGA 911 guarantees maximum end-to-end jitter across the network by designing a solution that utilizes NetFlow to analyze per packet performance. NGA 911 has a threshold of <15ms during a 15s interval. The SD-WAN deployed by NGA 911 is able to segment and individually differentiate and calculate the jitter of each carrier's networks. The primary fiber links will exceed the <15ms during a 15s interval criteria and are always set as the primary links for traffic on the network. Wireless and other supplemental or failover links have higher tolerance and range up to 30ms of jitter per 15s interval. Acceptance of this variance is in line with best practices in terms of preferring a quality link sufficient of delivering media without perceptible quality impairments over losing a link completely. Failure to meet the SLA objective for one month shall result in a 10% credit/or adjustment of the Total Monthly Recurring Cost (TMRC) of the fiber circuits that exceed the jitter threshold of <15ms during a 15s interval under contract for that month. Next consecutive month failure to meet the SLA objective shall result in a 20% credit/or adjustment of the TMRC of the circuits that exceed the jitter threshold of <15ms during a 15s interval under contract for that month. Each additional consecutive month failure to meet the SLA objective shall result in a 50% credit/or adjustment of the TMRC of the circuits that exceed the jitter threshold of <15ms during a 15s interval under contract for that month. NGA 911 uses a combination of NMS, MIS, logs, SNMP traps and algorithms to collect, collate, analyze and report on KPIs through our Web-based Portal. System and Network event logging are part of the NMIS and statistics and data related to events such as processor, ports, software (operating system errors, database errors, application errors and failures), network (quality of service [QoS], mean opinion score [MOS], jitter, latency, and packet loss) are measured, logged, analyzed and available for viewing on the Executive Dashboard and OSS interfaces. Reports are available on a daily, weekly, monthly, quarterly, annual, and custom basis and accessed from the NGA 911 Reports Engine.				

Any additional documentation can be inserted here

	Service Level Agreements - System Performance **Network Traffic Convergence** Specify convergence protocols and the estimated or guaranteed network convergence time (less than 54 ms) of IP traffic at any point within the proposed solution, including how convergence information will be gathered, calculated and provided to the Commission and affected PSAPs monthly or as requested.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			

SLA 9

Bidder Response:

Network convergence in the sense of call flow is the amount of time that network elements take over for failed components specifically related to media performance and depends on where in the network an event occurs. As described in more detail below, NGA 911's network traffic convergence is less than 54 ms and ranges from 9.6 to 50 ms.

Regarding convergence, there are three segments of the network to consider:

- NG Trunk Network
- NGCS or Core Network
- BCF/SBC

NG Trunk Network

The NG Trunk network provides the Ingress and Egress plumbing where Ingress is defined as the OSP traffic into the NGCS and Egress defines the NGCS to PSAP traffic. NGA 911's design leverages a minimum of three connections per NG Trunk. These trunks are configured on a 1500 MTU frame format for which each frame is monitored in real-time for optimal performance. Degradation or loss of a channel in the trunk is dedicated and accommodated in a range of 9.6 to 28.8 ms by utilizing packet sidecars. Network convergence at the NG Trunk is measured by time from the final (last) link is down and any other link picks up the traffic through the same SD-WAN or the H/A pair of the SD-WAN.

NGCS

The NGCS is made up of NENA FE's in two Regions and 4 AZ's that are linked by stateful databases. For an FE in our network, a loss of an element depends on the function, and is replaced or rerouted in real-time depending on TCP windows and SIP responses or lack thereof. These are not technically considered network traffic flows and instead are related to session initiation and maintenance. The case where an FE failure impacts the media path (which is not in all cases), a re-INVITE is sent to update the call path where network

	convergence does not exceed 50ms. Network convergence at the NGCS is measured by time from the final (last) FE is down and any of the remaining 7 FEs takes on the task. (note: by design there is zero downtime for such an occurrence.) **BCF/SBC** The SBC anchors traffic from the OSPs ingressing the network. Any change of network media traffic is dependent on negotiating with the SBC handling the traffic. For this reason, we have established a minimum of two SIP Aggregation points per OSP. NGA 911's SBCs are supported by a stateful database whereby, if supported by the OSP, a session media anchor can be moved between them using the same mechanism described for an NGCS FE above. Failure to meet the SLA objective for one month shall result in a 10% credit/or adjustment of the Total Monthly Recurring Cost (TMRC) of the functional element (FE), trunk or BCF that exceed the network convergence threshold of 54 ms under contract for that month. Next consecutive month failure to meet the SLA objective shall result in a 20% credit/or adjustment of the TMRC of the functional element (FE), trunk or BCF that exceed the network convergence threshold of 54 ms under contract for that month. Each additional consecutive month failure to meet the SLA objective shall result in a 50% credit/or adjustment of the TMRC of the functional element (FE), trunk or BCF that exceed the network convergence threshold of 54 ms under contract for that month. NGA 911 uses a combination of NMS, MIS, logs, SNMP traps and algorithms to collect, collate, analyze and report on KPIs through our Web-based Portal. System and Network event logging are part of the NMIS and statistics and data related to events such as processor, ports, software (operating system errors, database errors, application errors and failures), network (quality of service [QoS], mean opinion score [MOS], jitter, latency, and packet loss) are measured, logged, analyzed and available for viewing on the Executive Dashboard and OSS interfaces. Reports are available on a daily, weekly, monthly, quarterly, annual, and custom basis and accessed from the NGA 911 Reports Engine.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 10	**Service Level Agreements - System Performance** **Mean Time to Repair (MTTR)** Specify the MTTR characteristics of the proposed solution. These specifications shall reflect the end-to-end solution, as well as components or subsystems that are subject to failure. Include how MTTR information will be gathered, calculated and provided to the Commission and affected PSAPs.	X			

Bidder Response:

For all elements in the cloud (the NGCS) and the ESInet which are offered as service contracts, MTTR is not a measurable characteristic. Rather the NGCS and ESInet are measured by their overall Availability which is five nines.

The following equipment is installed at data centers, IXCs, POIs, the Host Sites and have a mean time to repair. This equipment is supplied and supported by our local partner. The switches, routers, controllers, and PDU are all actively monitored by our Network Management System and any errors in operation and malfunctions automatically logged. Each element can also be remotely rebooted if necessary. If there is maintenance, support, repair or replacement required these are reported and tracked in our ticketing system.

Equipment	MTTR (Hours)
Routers	12
Controller	12
Cables	12
PDU	2
Power System	2

	The status of equipment along with the virtual components of the NGCS and ESInet are provided to Nebraska Public Service Commission as part of our regular reporting method. ESInet components such as the NIDs, switches, routers, fiber, IXCs, and other facilities are provided as a service to NGA 911. Their individual performance and MTTRs are contractually structured so that the overall service availability exceeds 99.999% (see availability SLA below). NGA 911 has designed and architected the solution and certifies its performance for both the Nebraska Public Service Commission and in accordance with the FCC's Reliability Order. System and Network event logging are part of the NMIS and statistics and data related to events such as processor, ports, software (operating system errors, database errors, application errors and failures), network (quality of service [QoS], mean opinion score [MOS], jitter, latency, and packet loss) are measured, logged, analyzed and available for viewing on the Executive Dashboard and OSS interfaces. Reports are available on a daily, weekly, monthly, quarterly, annual, and custom basis and accessed from the NGA 911 Reports Engine.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 11	**Service Level Agreements - System Performance** **Mean Time Between Failures (MTBF)** Specify the MTBF characteristics of the proposed solution. These specifications shall reflect the end-to-end solution, as well as components or subsystems that are subject to failure. Include how MTBF information will be gathered, calculated and provided to the Commission and affected PSAPs.	X			
	Bidder Response: The following equipment is installed at data centers, IXCs, POIs, the Host Sites and have a measurable mean time between failure. This equipment is supplied and supported by our local partner. The routers, controllers, and PDU are all actively monitored by our Network Management System and any errors in operation and malfunctions automatically logged. Each element can also be remotely rebooted if necessary. If there is a maintenance, support, repair or replacement required these are reported and tracked in our ticketing system.				

Equipment	MTBF (Years)	Failures (per million hours)	MTTR {Hours}	Reliability
Routers	30	3.8	4	99.995%
Controller	50	2.3	4	99.997%
Cables	500	0.2	12	100.000%
PDU	40	2.9	4	99.999%
Power System	30	3.8	4	99/995%
		Individual Equipment (Aval)-not system availability which is > 5' 9s		99.9%

Annual Down Time components (not sys)	**48 minutes**

Annual Down Time for the end to end system with redundancy	**<5 minutes**

NGA 911 uses a combination of NMS, MIS, logs, SNMP traps and algorithms to collect, collate, analyze and report on KPIs through our Web-based Portal. System and Network event logging are part of the NMIS and statistics and data related to events such as processor, ports, software (operating system errors, database errors, application errors and failures), network (quality of service [QoS], mean opinion score [MOS], jitter, latency, and packet loss) are measured, logged, analyzed and available for viewing on the Executive Dashboard and OSS interfaces.

Reports are available on a daily, weekly, monthly, quarterly, annual, and custom basis and accessed from the NGA 911 Reports Engine.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 12	**Service Level Agreements - System Performance** **Network Reliability** Network reliability is defined as the ability for system end-points to effectively communicate with each other, and all associated data and information is exchanged in usable formats. An IP-based network looks at reliability as an overall redundancy design, rather than component by component. Specify in the response the overall reliability service level of the IP network, including all bidder-provided components and facilities.	X			

Bidder Response:

NGA 911 provides the Nebraska Public Service Commission an SLA for Public Safety Grade ESInet and NGCS.

Public Safety Grade

NGA 911 designs, engineers and deploys the ESInet and the NGCS to exceed Public Safety Grade as defined in Section V.D.1.b. of the RFP. As noted in the Section, The term "public safety-grade" has been utilized to refer to this level of standards compliance; however, a universal definition of this term has not been proposed by a Standards Development Organization (SDO). The industry accepted standard for public safety grade systems and networks is five nines (99.999%). NGA 911 exceeds 99.999% reliability and availability as a matter of course. NGA 911 never relies on a single network service provider for ESInet connectivity. We aggregate and bond broadband trunk circuits from at least 3 providers.

ESInet - Ingress and Access Networks

NGA 911 exceeds the PSG requirement through our diverse engineering of the "last mile" by being carrier agnostic and seeking geographically and carrier diverse networks. . As a result, NGA 911 is able to leverage state and commercial assets. NGA 911's primary concern is the value of survivability, reliability, and connectivity of the network. NGA 911 never settles for the status quo and will constantly, through the term of the contract, look to leverage existing assets to provide better performance to the state of Nebraska.

NGA 911 is providing a High Availability (H/A) SD-WAN interface solution to all Endpoints (PSAPs, Aggregation Points, and Direct Connect Facilities). The SD-WAN seamlessly bonds diverse IP based interconnections (WANs) into a single integrated connection. The SD-WAN handles BGP (Layer 2 or Layer 3) at each PSAP and at additional points based on mutually agreed connections to the data centers. The SD-WAN is transport independent and is centrally managed by NGA 911. It offers a shared VPN schema across any WAN circuit (i.e. Microwave, LTE, MPLS, broadband, etc.) and supports flexible VPN extension to all endpoints (IaaS, Host, Host Data Centers) with a supporting SD WAN appliance.

	The SD-WAN technology deployed end-to-end by NGA 911 appends flow tracing packets to each and every packet traversing the whole ESInet from ingress to egress whether signaling or media. These "sidecars" are used to measure latency, jitter, route, and travel times for each and every route and interconnect service provider on the net. This includes signaling (meta data); media information such as codec and protocol; network performance logs for latency, jitter, and packet loss; and Mean Opinion Score (MOS) and other quality indicators of fidelity. The logging begins from ingress as a call is received from an Originating Service Provider (OSP). Any transcoding is noted and validated. A MOS score is recorded at ingress to be used for comparison at egress. Additionally, the SD-WAN binds the diverse provider's connections into dual aggregate connections that permit a media comparator function. The real time and historical data gathered from the SD-WAN offer an unprecedented view of the overall and specific network service provider performance allowing SLA's to be managed and enforced. The NGA 911 NGCS requires Firewalls as part of the BCF/SBC functions. The SD-WAN includes a Zone-based, Stateful firewall. NGA 911's service also includes Zscaler for Deep Package Inspection (DPI) on the cloud. NGA 911 will also provide additional firewall solutions when needed as part of our defense in depth security package. NGA 911 uses a combination of our NMS, MIS, logs, SNMP traps and algorithms to collect, collate, analyze and report on KPIs through our Web-Based Portal. System and Network event logging are part of the NMIS and statistics and data related to events such as processor, ports, software (operating system errors, database errors, application errors and failures), network (quality of service [QoS], mean opinion score [MOS], jitter, latency, and packet loss) are measured, logged, analyzed and available for viewing on the Executive Dashboard and OSS interfaces. Reports are available on a daily, weekly, monthly, quarterly, annual, and custom basis and accessed from the NGA 911 Reports Engine.

Any additional documentation can be inserted here

SLA 13	**Network Availability** 1. Specify the service level offered as a percentage of time when the service is available, and the maximum period of total outage before remedies are activated. Availability is defined as MTBF/(MTBF+MTTR). 2. Include how system availability information will be gathered, calculated and provided to the Commission and affected PSAPs.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: 1. The overall SLA for the NGA 911 network availability is 99.999% Individual components have less than 99.999% availability; however all components in the network are deployed with redundant components or carriers. Considering MTBF/(MTBF + MTTR) the following individual equipment uptimes are calculated. PLEASE NOTE these are uptimes for individual components and NOT the system as a whole for which additional redundancy is provided. In other words, even if one router fails and then is replaced (according to the table below at a reliability of 99.995%) there is another router still operating – so overall availability of the redundant system still exceeds 99.999%.				

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

Equipment	MTBF (Years)	Failures (per million hours)	MTTR {Hours}	Reliability
Routers	30	3.8	4	99.995%
Controller	50	2.3	4	99.997%
Cables	500	0.2	12	100.000%
PDU	40	2.9	4	99.999%
Power System	30	3.8	4	99.995%
		Availability (per component -not system)		99.9%
		Annual Down Time (per component)		48 minutes

Annual Down Time for the network with redundancy	<5 minutes

	2. The status of this equipment is collected by our NMS (using SNMP) and along with the virtual components of the NGCS and ESInet are provided to the State of Nebraska and its PSAPs as part of our regular reporting methods. System and Network event logging are part of the NMIS and statistics and data related to events such as processor, ports, software (operating system errors, database errors, application errors and failures), network (quality of service [QoS], mean opinion score [MOS], jitter, latency, and packet loss) are measured, logged, analyzed and available for viewing on the Executive Dashboard and OSS interfaces. Reports are available on a daily, weekly, monthly, quarterly, annual, and custom basis and accessed from the NGA 911 Reports Engine.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 14	**Service Level Agreements - System Performance** **End-of-Support Equipment** Contractor shall proactively replace, at Contractor's expense, any hardware that has reached end of support (EOS) no later than 90 calendar days prior to the manufacturer's EOS date. All equipment must be new and of current manufacture, not refurbished. Describe your procedures for End-of-Support Equipment.	X			
	Bidder Response: NGA 911 proactively replaces any hardware and software at least 90 days prior to it's EOS date. NGA 911 maintains a complete inventory of all equipment and software and monitors closely all EOS notifications from the manufacturers. NGA 911 will identify all EOS components and create a planned replacement strategy for the hardware and software. NGA 911 will notify the Commission when the replacements are scheduled. NGA 911 is a managed service solution and will perform this service at no additional cost to the State or PSAP. All equipment deployed by NGA 911 is new. The NGA 911 procedure for End-of-Support Equipment is similar to any maintenance for hardware/software upgrade and/or replacement. NGA 911 will provide release notes to the Commission and PSAP a minimum of 45 days before implementation. This documentation details the deployment process and timeline for scheduled and maintenance releases. Also, a description of how releases shall be tested within the ESInet and NGCS. As a standard, maintenance and service events are planned for Monday through Thursday between the hours of midnight and 4 AM local time. However, NGA 911 will work with the State of Nebraska PSAPs to define the Public Safety Maintenance Window that is most appropriate for them – based on PSAP operations. NGA 911 will work with the State of Nebraska to review the following types of information to determine the most appropriate scheduling for all serviceable events. The types of information include: • Busy hour calculations • Busy day calculations • Local planned and special events • Local planned Police Department and Sheriff's Office events • PSAP resources • Weather NGA 911 Operations Staff will make advance notification of planned maintenance work to the State of Nebraska PSAPs. Notification will depend on the event type and will occur a minimum of 7 days in advance for all core hardware replacement events and a minimum of 48 hours in advance for all general serviceable events. Notification will occur via email and other formats, as agreed.				

	NGA 911 Operations Staff will confirm receipt of notification and approval of the day and time for the event in advance. In addition, prior to initiation of any event, State of Nebraska/PSAP personnel will be requested to confirm that call volume is acceptable for a serviceable event and that there are no critical issues under management at that time. Should the serviceable event be critical in nature, the initiation time will be managed with the State of Nebraska/PSAP to ensure resolution of the critical issue in a timely manner.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 15	**Service Level Agreements –** **SLAs for Incident Management** The Commission requires the Contractor to establish processes and procedures for supporting a NOC/SOC that can rapidly triage and manage reported network incidents. Bidder shall develop an ITIL compliant severity-level scale that includes levels one through four, with level one being the most severe incident. The top two levels shall capture all incidents affecting the level of service of one or more end-points. Include a description of incident severity-level attributes, including response and resolution times for each severity level, and how response and resolution times are measured.	X			

Bidder Response:

In order to maintain optimal router, switch, and functional element configurations, NGA 911 adheres to the continuous assessment model to rapidly triage and manage network incidents. Build types are based on Customer Needs, Enhancements, and on Operational Necessity. Each type is coded in an Agile manner and integrated into the Test Environment. After successful testing, the releases are delivered in the parallel active-active manner described above. Utilizing the capabilities of our NOC/SOC software defined WAN; direct and immediate comparisons are made between the new load and current release. Performance is verified on a number of metrics including end-to-end jitter, latency, MOS fidelity, and call response times for both.

NGA has defined an ITIL compliant severity-level scale as further specified in NOC/SOC 11. It includes levels one through four, with level one being the most severe incident. The top two levels shall capture all incidents affecting the level of service of one or more end-points. Our ITIL includes a description of incident severity-level attributes, including response and resolution times for each severity level, and how response and resolution times are measured

Any findings or measurements that fall out of the specified norm for the new release result in an automatic restoration to the current release.

The key features of the Transaction Database Service for the Public Service Commission are the following:

- Highly durable – Volumes are divided into 10 gigabyte (GB) segments; each segment is replicated six ways across three Data Centers.

- Fault-tolerant – It transparently handles the loss of up to two out of six data copies without losing write availability or three out of six copies without losing read availability.

- Self-healing – It monitors disks and nodes for failures and automatically replaces or repairs the disks and nodes without the need to interrupt read or write processing from the database node.

	● Storage autoscaling – It automatically grow the size of the database volume as storage needs grow. The volume will grow in increments of 10 GB up to a maximum of 64 TB. ● Continuous backup – Backups are automatic, incremental, and continuous and have no impact on database performance. Automated backups are stored in File Services (detailed below), which is designed for 99.999999999 percent durability. ● Read replicas – Each cluster can have up to 15 read replicas across multiple Data Centers to scale out read operations or act as failover targets. The replicas share the same data volume as the primary instance, and replication lag is very low, typically in the tens of milliseconds. ● Highly secure – Uses Secure Sockets Layer (SSL) to secure data in transit as well as encryption of data at rest. NGA 911 uses a combination of our NMS, MIS, logs, SNMP traps and algorithms to collect, collate, analyze and report on KPIs through our Web-Based Portal. System and Network event logging are part of the NMIS and statistics and data related to events such as processor, ports, software (operating system errors, database errors, application errors and failures), network (quality of service [QoS], mean opinion score [MOS], jitter, latency, and packet loss) are measured, logged, analyzed and available for viewing on the Executive Dashboard and OSS interfaces. Reports are available on a daily, weekly, monthly, quarterly, annual, and custom basis and accessed from the NGA 911 Reports Engine.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 16	**Service Level Agreements –** **Outage Notification and Reason for Outage (RFO) Report** **Outage Summary and Lessons Learned** Provide a summary of FCC reportable outage situations that interrupted 911 service to bidder's clients over the past three years, where 911 calls were not delivered or not delivered to the appropriate PSAP as a result of the issue. The response shall include the deployment type (legacy, ESInet, and NGCS), month, year, duration, number of PSAPs or population impacted, number of PSAPs or population served by the impacted system, impacted system, and lessons learned from each outage. **Regulatory Compliance** Contractor shall comply with all applicable local, state, and federal outage and notification rules throughout the term of the contract.	X			
	Bidder Response: NGA 911 nor our clients have experienced an FCC reportable outage situation that interrupted 9-1-1 service over the past three (3) years. NGA 911 will comply with all applicable local, state, and federal outage and notification rules throughout the term of the contract. NGA 911 is registered with the FCC Network Outage Reporting System (NORS).				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 17	**Service Level Agreements –** **Outage Notification and Reason for Outage (RFO) Report** **Outage Notification** Contractor shall notify the Commission and affected PSAPs within a maximum 30 minutes of discovering an event or outage that may impact 911 services. All events that meet criteria for local, state, or federal reporting shall also be completed by the Contractor. At the time of initial notification, the Contractor shall convey all available information that may be useful in mitigating the effects of the event or outage, as well as a name, telephone number, ticket or reference number, and email address at which the service provider can be reached for follow-up. The Contractor is responsible for coordinating data gathering, troubleshooting and reporting on behalf of bidder's subcontractors. Describe how the solution meets or exceeds the above requirements.	X			

Bidder Response:

Notification

NGA 911 will notify the Commission and impacted PSAPs, and/or designated agencies within 30 minutes of discovering an event or outage that may impact 9-1-1 services in Nebraska by email, voice, and/or text. NGA 911 has an established protocol for incident notifications. At the time of initial notification, the NGA 911 NOC/SOC will provide the unique incident number, date and time opened, status of the ticket, and description of the problem, geographical location, agencies impacted, and type of service-impacting event. NGA 911 will provide mitigation options for the event or outage, as well as a name, telephone number, ticket or reference number, and email address at which NGA 911 can provide follow-up.

NGA 911 complies with all local, state, and the FCC Network Outage Reporting System (NORS).

Communications

NGA 911's Incident Management System (IMS) automatically sends email updates to the Commission and PSAP members whenever a change is made to the incident, including all notes made to the tracking log, priority level changes, and incident closure. Additionally, a Technical Service Representative will be assigned to monitor and notify the Commission and PSAP via telephone with updates.

The NGA 911 IMS will provide automatic notification and NOC/SOC personnel will notify the Commission and PSAPs by phone per the following SILs of any outage.

NGA 911 has clearly defined processes that include an Escalation Matrix, Prioritization, and Incident Handling protocols.

Rank and SLA	Level 1 Critical	Level 2 Major	Level 3 Minor	Level 4 Standard
Response/ Acknowledge	< 15 minutes	< 30 minutes	8 hours	Based on request
Tech on Site (if required)	0-2 hours	2 hours	Next Business Day	Based on request
Escalation Threshold	1 hour	2 hours	48 hours	As needed
Communication Objective	Hourly	Every 2 hours	Daily	As needed

Severity Level 1: Critical Impact/System down

Examples including but not limited to:

- The entire system, or an entire subsystem failure
- Network failure to the PSAP
- Any factor that prevents call movement at ingress or egress
- Catastrophic Building fault e.g. flooding

Response Time: Initial response is under 30 minutes (any time of day). Problem will be addressed hourly until the system is restored to a functional and mutually agreeable state pending a permanent fix. If a catastrophic (hardware or software) fault is found with the

equipment/system, this correction will be addressed immediately. NGA 911 will provide a correction for software or hardware (Replacement, Replace, or Recall) as required to restore the system to operation.

Severity Level 2: Significant Impact

Examples including but not limited to:

- Occasional service interruptions
- System operations can be recovered by manual intervention
- Major system features or functions are affected
- A redundant component failure but system is operational

Response Time: Initial response under 30 minutes (any time of day). Problem will be addressed every 2 hours/per day until the system is restored to a functional and mutually agreeable state pending a permanent fix.

Severity Level 3: Normal/Minor Impact

Examples including but not limited to:

- The failure restricts use of a capability
- Non-critical function affected

A redundant part of the hardware or software has failed, and the system is still operating completely, however, without backup.

Response Time: This level of severity will be addressed in 8 hours. If a maintenance software release, or a hardware bulletin to address this issue the ticket may not be resolved in 48 hours. Any new features the Customer may request will be addressed individually outside of this agreement.

	Severity Level 4: Low/Informational Examples including but not limited to: · The failure results in an acceptable workload · Prevents or restricts use of a non-essential capability and can be handled procedurally · Product enhancement not service affecting Response Time: This level of severity will be addressed within 96 hours during business hours. A technical bulletin may result. Any new features the Customer may request will be addressed individually outside of this agreement.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 18	**Service Level Agreements –** **Outage Notification and Reason for Outage (RFO) Report** **Status Updates** The Contractor shall communicate any updated status information to the Commission and affected PSAPs no later than two hours after the initial contact, and at intervals no greater than two hours thereafter until normal 911 service is restored. This information shall include the nature of the outage, the best-known cause, the geographic scope of the outage, the estimated time for repairs, and any other information that may be useful to the management of the affected operations. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: NGA 911 will notify the Commission and impacted PSAPs, and/or designated agencies no later than two (2) hours after the initial event or outage that may impact 9-1-1 services in Nebraska and will provide regular updates at intervals no greater than two hours until the 9-1-1 service is restored. At the time of initial notification, the NGA 911 NOC/SOC will provide the unique incident number, date and time opened, status of the ticket, and description of the problem, geographical location, agencies impacted, and type of service-impacting event. NGA 911 will provide mitigation options for the event or outage, as well as a name, telephone number, ticket or reference number, and email address at which NGA 911 can provide follow-up.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 19	**Service Level Agreements –** **Outage Notification and Reason for Outage (RFO) Report** **Reason For Outage (RFO) Reporting** Following the restoration of normal 911 service, Contractor shall provide a preliminary RFO report to the Commission and affected PSAPs no later than three (3) calendar days after discovering the outage. An in-depth RFO report, including a detailed root-cause analysis, shall be provided to the Commission and affected PSAPs no later than ten (10) calendar days after discovering an outage. 1. Describe how bidder will comply with the notification and reporting requirements above. 2. Describe the NOC/SOC tools and techniques at bidder's disposal to ensure that bidder's various subcontractor perform troubleshooting and post-event analysis and provide associated reports.	X			
	Bidder Response: NGA 911 will provide a written preliminary RFO report to the State no later than three (3) calendar days. Additionally, NGA 911 will provide an in-depth RFO report, and detailed root-cause analysis (RCA) to the Commission and affected PSAPs no later than ten (10) calendar days (or as otherwise agreed to by the Commission) after restoration of normal 9-1-1 services. A conference call option is available to the Commission to discuss the results of the RFO at any time. 1.The NGA 911 SOC/NOC trouble ticketing systems are electronically bonded (e-Bonding) with all service providers supporting the ticketing system. The e-Bonding of ticketing systems allows near real-time notification of issues, status and the capability of tracking or sharing of information during an outage and the restoration processes between the SOC/NOC and the supplier. The SOC/NOC is responsible for communicating this information to the Commission and the PSAP. NGA 911 is responsible for providing the consolidated RFO to the Commission. NGA 911 is registered with the FCC Network Outage Reporting System (NORS). See diagram below. 2. NOC/SOC - NGA 911 takes security and monitoring very seriously, through our NOC/SOC we have 24x7x365 monitoring of our solution proposed for the State of Nebraska. NGA 911 provides near real-time alerts when the monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by service and Security teams. NGA 911 correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis. Upon assessment and discovery of risk, we disable accounts that display atypical usage matching the characteristics of bad actors. Our Security team extracts all log messages related to system access and provides reports to designated officials. Log analysis is performed to identify events based on defined risk management parameters. The NGA 911 has a comprehensive security plan outlined below: 1. Preparation 2. Detection of Even				

	3. Notification 4. Activate an Incident Response Program 5. Triage and Containment 6. Response Plans 7. Remediation 8. Notification

Step	Type	Description	Who
1	Open Communication Event	Open Communication Event. Provide a description of the issue and specify the level of assistance expected from technical personnel to resolve service-related issues.	Create a community of Stakeholders including Technical Personnel and other entities, NGA 911 Operations Support Manager and Project Manager.
2	Send Email	Send notification email of Communication Event Open.	To all identified Stakeholders
3	Event Logging	In order to maintain a complete historical record of all issues all relevant details must be maintained in the Communication Event	The Owner of the Event should ensure all records are accurate.
4	Event Investigation/Diagnosis	The Owner will determine the best method to resolution which may include one or more of the following: Email, in-person meeting, webinar, Conference Call	The Owner of the Event should identify the method of communication and initiate discussions.
5	Event Resolution	Technical Staff should attempt to resolve any issues in collaboration with NGA 911.	All impacted Stakeholders
6	Event Closure	Event Owner should confirm that the event has been resolved and all impacted Stakeholders are satisfied and in agreement.	Event Owner

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 20	**Service Level Agreements –** **Outage Notification and Reason for Outage (RFO) Report** **PSAP Notifications** Outage notifications and follow-up analysis of outages are a critical element to understanding overall system health and preventing future service interruptions. Having awareness of issues that exist in a neighboring PSAP provides valuable insight into potential issues that may begin impacting another PSAP's operations. The Commission is seeking an outage notification service that allows for each PSAP to elect the outage notification types and PSAPs for which it will receive outage notifications, outage updates and RFO reports. A web portal for authorized users to select/deselect outage notifications is required. Provide a detailed description of how bidder will support such an outage notification service.	X			
	Bidder Response: Through monitoring of all Functional Elements, NGA 911 will be able to quickly identify and respond to alarms and network events in the network for the PSAP and neighboring PSAPs on the ESInet. The NGA 911 Web-Portal Management allows for customization of end user notifications. The PSAP and/or State administrators can configure who gets access as well as who has access to what data. Account administrators are provided with full control over every adjustable feature within the Administrative Web-Portal settings including outage notifications and follow up analysis of outages. Once the account administrator has given access to an end user, the end user will need to login and build a profile. This profile will include notification preference, types of outage notification, outage updates and RFO reports. NGA 911's IMS has the ability to provide updates by automated email and text. Additionally, NGA 911's Network Operations Center will make direct notification by phone to the State and entities with connectivity to the ESInet and NGCS solutions. The NGA 911 Incident Management System (IMS) generates tickets for automated alarms and network events as well as allows for the PSAP and ISP to open trouble tickets. All tickets and ticket updates are automatically sent to the State and identified affected users. Anyone in receipt of event notification can opt out of event notification by incident by replying to the email or by phone call to the NOC requesting to opt out of notifications. NGA 911 will send notifications not only to predetermined state personnel and PSAP contacts, at a minimum of one per PSAP, but also to any additional requested entity. This request can be made by email or via a call to the NGA 911 NOC.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 21	**Service Level Agreements –** **Media Contact** 1. Contractor shall provide a 24 x 7 spokesperson who will be available for media contact regarding ANY outage of 911 service due to any failure of 911 call delivery to the Commission's host equipment and to the affected PSAPs. **Government & Regulatory Contact** 2. Contractor shall provide a 24 x 7 representative who will be available for government and regulatory contact regarding ANY outage of 911 service due to any failure of 911 call delivery to the Commission's host equipment and to the affected PSAPs Describe bidder's experience in providing both a Media Contact and Government & Regulatory Contact for similar contracts.	X			
	Bidder Response: **Media Contact** 1. NGA 911 will provide the Commission and PSAP a 24x7x365 spokesperson who will be available for media contact regarding ANY outage of 9-1-1 service due to any failure of 9-1-1 call delivery to the Commission's host equipment and to the affected PSAPs. **Government & Regulatory Contact** 2. NGA 911 will provide a 24x7x365 representative who will be available for government and regulatory contact regarding ANY outage of 9-1-1 service due to any failure of 9-1-1 call delivery to the Commission's host equipment and to the affected PSAPs NGA 911's Media Contact has been in the industry for over 15 years and our Government & Regulatory Contact has been in the industry for 27 years. NGA 911 will provide all contact information 30 days prior to the first PSAP Go Live cut.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 22	**Service Level Agreements –** **SLA Violations** An SLA violation shall have occurred whenever: A. The Contractor fails to meet any single performance level; or, B. The average of any single performance item over the preceding two-month period fails to meet the service level stated in response to requirements SLA 1 through SLA 21. Contractor shall deliver an SLA violations report to the Commission on a monthly basis. **SLA Reporting** Provide a detailed description of how bidder measures and reports incidents, including immediate notifications and regularly scheduled reports. SLA results shall be delivered to the Commission on the 10th business day of the month. The report shall include all performance items identified in the bidder's proposal and documented in contract negotiations.	X			

Bidder Response:

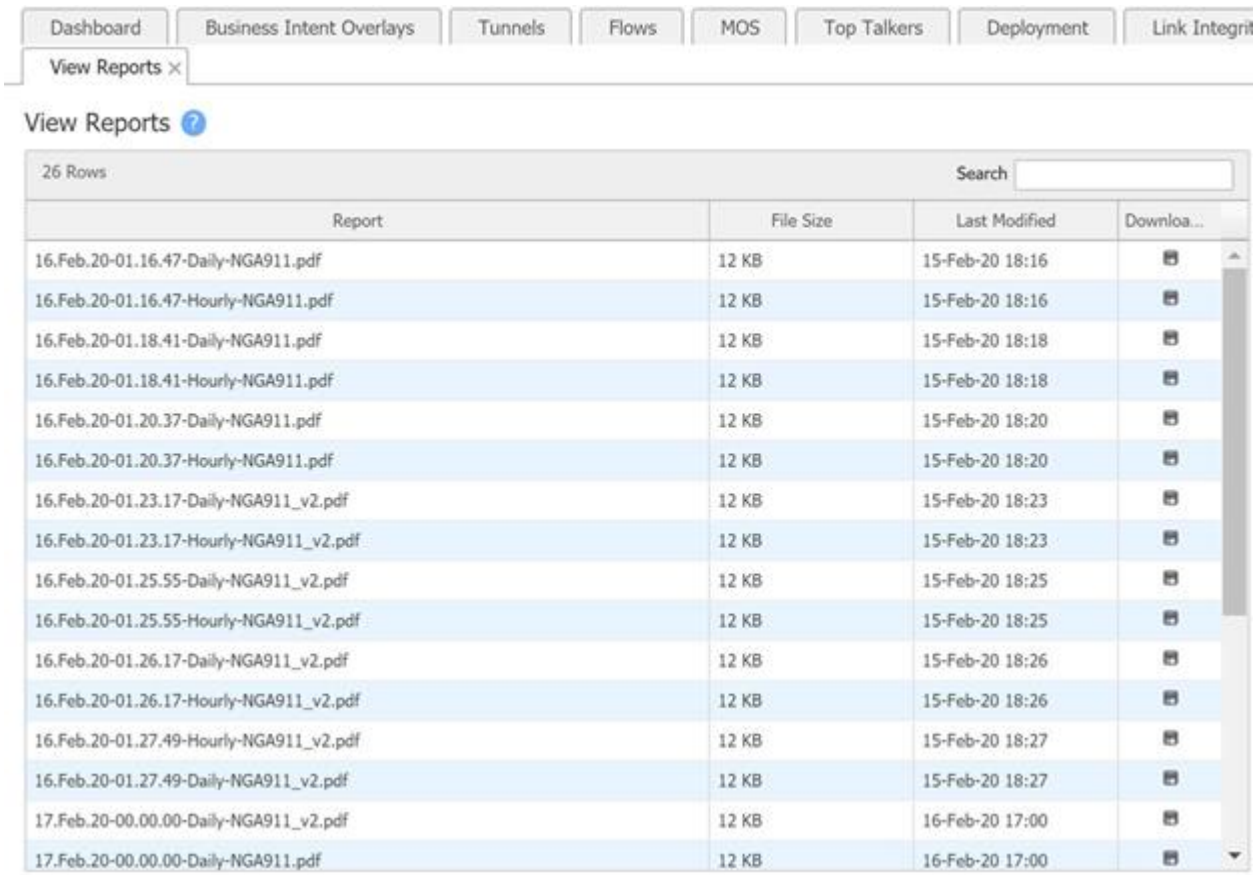
Measurement

NGA 911 uses open source standards based active-active architecture that leverages Bidirectional Forwarding Detection (BFD) as well as packet-by-packet inspection of the media traffic (multi pathed options) and adheres to the BFD protocol as defined in IETF RFC 5880 and RFC 5881 or other standards-based, non-proprietary methods approved by the State for measuring incidents. We are recommending that the State take advantage of open source and trends in the industry that leverage NetFlow and SD-WAN technologies.

For example, Netflow probes in the network measure and monitor bandwidth, latency, jitter, packet loss, QoS and VoIP MOS end-to-end and at the element level. Additionally, sidecars that transit the network are accessed through the OSS for security monitoring, performance monitoring, troubleshooting and maintenance. SLA's from all supporting vendors and AWS are entered into the network monitoring rules engine for validation and accounting. Separate probes are in place for monitoring of the Kamailio and Freeswitch functions of the NGCS at the application and networking layer. Infrastructure monitoring focuses on the physical elements in the hardware elements in the cloud including ec2, S3, Aurora, Docker Containers.

If NGA 911 detects an incident that falis our SLAs 1 through SLA 22 the system automatically alerts and provides required analytics for reporting.

Communication
If NGA 911 has a single performance item over the preceding two-month period that causes our solution to fail to meet the service levels in SLA 1 through SLA 22 we will deliver an SLA violation report to the Commission on a monthly basis.



Report	File Size	Last Modified	Downloa...
16.Feb.20-01.16.47-Daily-NGA911.pdf	12 KB	15-Feb-20 18:16	
16.Feb.20-01.16.47-Hourly-NGA911.pdf	12 KB	15-Feb-20 18:16	
16.Feb.20-01.18.41-Daily-NGA911.pdf	12 KB	15-Feb-20 18:18	
16.Feb.20-01.18.41-Hourly-NGA911.pdf	12 KB	15-Feb-20 18:18	
16.Feb.20-01.20.37-Daily-NGA911.pdf	12 KB	15-Feb-20 18:20	
16.Feb.20-01.20.37-Hourly-NGA911.pdf	12 KB	15-Feb-20 18:20	
16.Feb.20-01.23.17-Daily-NGA911_v2.pdf	12 KB	15-Feb-20 18:23	
16.Feb.20-01.23.17-Hourly-NGA911_v2.pdf	12 KB	15-Feb-20 18:23	
16.Feb.20-01.25.55-Daily-NGA911_v2.pdf	12 KB	15-Feb-20 18:25	
16.Feb.20-01.25.55-Hourly-NGA911_v2.pdf	12 KB	15-Feb-20 18:25	
16.Feb.20-01.26.17-Daily-NGA911_v2.pdf	12 KB	15-Feb-20 18:26	
16.Feb.20-01.26.17-Hourly-NGA911_v2.pdf	12 KB	15-Feb-20 18:26	
16.Feb.20-01.27.49-Hourly-NGA911_v2.pdf	12 KB	15-Feb-20 18:27	
16.Feb.20-01.27.49-Daily-NGA911_v2.pdf	12 KB	15-Feb-20 18:27	
17.Feb.20-00.00.00-Daily-NGA911_v2.pdf	12 KB	16-Feb-20 17:00	
17.Feb.20-00.00.00-Daily-NGA911.pdf	12 KB	16-Feb-20 17:00	

NGA 911 can offer reports in a number of different formats. We will work with the Commission and PSAPs to select the reports and format that best convey the availability information succinctly and directly.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SLA 23	**Service Level Agreements –** **SLA Violation Financial Remedies** Contractor shall provide financial remedies to the Commission for each event in which service levels are not maintained. The Commission requires that all of the Contractor's network facilities, devices, and services will be measured on a rolling, 12-month calendar. Failure to meet SLAs shall be measured per service-affecting outage. Financial remedies shall be assessed for failure to meet SLAs. For service-affecting incidents, a 10 percent (10%) discount shall be accessed against the Monthly Recurring Charge (MRC) applicable to the source of the failure, whenever the initial period of resolution is exceeded. If the resolution period length of time doubles, then the discount shall increase to 20 percent of the MRC. If the resolution period length of time quadruples the initial period, then 50 percent of the MRC shall be assessed. The amount related to the damages is to be credited to the invoice for the month immediately following the violation. Bidder shall include how uptime information will be gathered, analyzed and provided to the Commission.	X			
	Bidder Response: SLA Violation Financial Remedies: For service-affecting incidents, a 10 percent (10%) discount will be accessed against the Monthly Recurring Charge (MRC) applicable to the source of the failure, whenever the initial period of resolution is exceeded. If the resolution period length of time doubles, then the discount shall increase to 20 percent of the MRC. If the resolution period length of time quadruples the initial period, then 50 percent of the MRC shall be assessed. The amount related to the damages is to be credited to the invoice for the month immediately following the violation. For each type of metric (KPI) defined above including but not limited to latency, jitter, loss, MOS, outage, etc defined above NGA 911 provides details on how uptime/downtime information is gathered, analyzed and provided to the Commission. Uptime is calculated based on the parameter and KPI' defined above for the end to end service as a whole. A service impacting incident is one where the measured parameter falls below the threshold and a redundant instance, component or parameter is not able to maintain the full SLA. service downtime/service uptime for the preceding month - where the criteria is an annual average.				

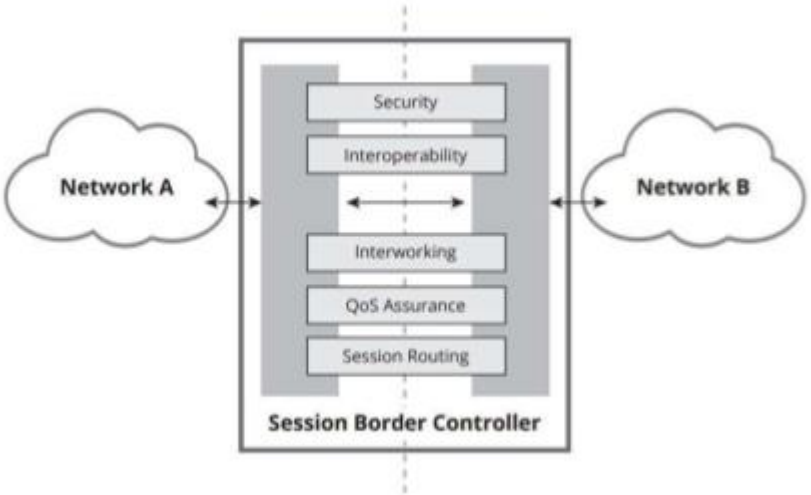
Any additional documentation can be inserted here

Operational Scenarios
Safeguards shall be established to minimize the impact of human or system error. Describe bidder's risk-mitigation and issue-resolution strategies for the following hypothetical scenarios:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN SCEN 1	**Scenario 1** At 0300 hours, a series of SBC alarms previously unseen by the NOC staff on duty begin to increase in volume and frequency. At 0330, multiple critical alarms are received. At 0345, a few PSAPs start reporting garbled audio while others report an inability to obtain location information. At 0600, some PSAPs are reporting that they have not received a call in the last 15 minutes.	X			

Bidder Response:

In this example, the 0300 hours SBC alarms will be first noticed at the Primary NOC in Houston, TX and the Secondary NOC in Chicago if not picked up by the Primary in a time consistent with the threat level. Even though they have not seen the particular alert before, they query the SBC to determine which interfaces, ports, and addresses are being impacted (if the alarm indicator did not provide this information). One level check is to assess the SBC's activity related to the SPOOFED calls. NGA 911 is sending a constant, but randomized series of known spoofed calls through the network at all times. These "pseudo" calls are used to measure end-to-end performance, jitter, latency, MOS quality, media, and signaling security. Since the spoofed "pseudo" call is of a known and measurable quantity and quality with random, but known, location, addressing, and authorization credentials (designed to cover the range of known attacks and/or system malfunctions), the NOC and support Tier III engineers can assess which set of spoofed calls, if any, are being impacted. The set of calls impacted varies on whether the SBC is experiencing a security compromise, malware, or other elements in the network related to end-to-end performance. This unique approach of using variable spoofed calls as a troubleshooting tool means that nearly all routine issues will be identified and corrected at Tier II or III before impacting the PSAP.



Despite this method and keeping with the scenario described, we must assume all of the spoofed "pseudo" calls are going through. Otherwise, NGA 911 would isolate and repair the issue at first report at 0330, and Tier III support would have identified the type of spoofed calls not going through and begun to focus on the culprit. In the situation at 0345, spoofed calls with certain location

	(PIDF-LO) attributes and voice codecs can be specifically run to test performance and identify which types and forms of codecs and location data are causing the problems. Simultaneously to the generation, monitoring, and ordering for testing purposes of spoofed calls, all routers, switches, and Ingress Network Elements from the LNG to direct i3 SIP interconnections with the OSPs are examined on a case by case basis to verify conformance with the expected Ingress patterns and SIP Header formats. Finally, since all elements are virtualized, they can be changed out with alternative stacks and containers until the problematic component is isolated and removed. NGA 911 utilizes Silver Peak and Darktrace as security overlays. Silver Peak allows for the measuring of known calls against the actual performance of the network. Darktrace uses AI to identify, catalog, and measure normal signal and traffic flow to identify and react to anomalies in the network before humans or legacy approaches identify an issue. These tools are part of the toolkit Network Management engineers will use to troubleshoot a specific issue. In the event of increasing alarms within the Session Border Controller (SBC), loss of the ability to perform outbound calls over the ESInet PSTN lines, or degradation of Quality of Service (QoS) without NGA 911 NOC acknowledgment, the State should contact the NGA 911 Help Desk Technician (HDT) to report any ongoing issues. An NGA 911 HDT shall open a trouble ticket on behalf of the Commission/PSAP member(s) reporting the issue in the NGA 911 Incident Management System (IMS) and provide an IMS trouble ticket number. NGA 911 HDT will immediately notify the NGA 911 NOC and NGA 911 Engineering team of the trouble being reported. NGA 911 HDT will verify that all 9-1-1 and non-emergency calls have been rerouted to the backup PSAP as per the Alternate Answer Plan provided by the Commission/PSAP. The NGA 911 HDT will request that the NGA 911 NOC begin troubleshooting the reported issue and verify that there is no outage with the Data Service Provider. If the NGA 911 NOC has verified that NGCS is in good working order the NGA 911 HDT will contact the Commission/PSAP member(s) to request that the Commission/State either open a trouble ticket with their CPE vendor or NGA 911 HDT will contact the vendor on behalf of the PSAP to correct any ongoing issues. NGA 911 HDT shall provide the Commission/PSAP member(s) or identified contact of trouble found along with the resolution and estimated time to restore service. The NGA 911 HDT shall also monitor the progress of the trouble ticket to verify that NGA 911 is following the NGA 911 Service Level Agreements (SLA) provided to the State. If the SLAs are not met in a timely manner, the NGA 911 HDT shall escalate eternally until the issue has been resolved. Additionally, any impacted person and other stakeholder with access to the NGA 911 Web-Portal can access the Trouble Ticket, and ongoing trouble log for real-time updates.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN SCEN 2	**Scenario 2** All originating service providers in the state are connected directly via Signaling System Number 7 (SS7) protocol to the bidder's LNGs that serve the PSAPs in Nebraska, as well as others outside the Commission's footprint. Each LNG consistently processes about 10,000 calls per day, but each is capable of processing in excess of 100,000 calls per day. One of the LNGs experiences a catastrophic failure and is unable to process any calls. In a review of the prior day's logs, it is found that the two surviving LNGs only are processing 2,000 calls each.	X			
	Bidder Response: In this scenario it would be a critical network event in which case the NGA 911 NOC would open a Severity 1 (service impacting) trouble ticket. The trouble ticket portal would automatically generate an email notification to the Commission/PSAP and the NGA 911 Executive Management Team, as well as any additional identified stakeholders notifying them of the issue. NGA 911 and our subcontractors would immediately initiate the process for a Severity 1 incident and engineers from all teams (911, IP Engineering, Tier 2, and Translations) would call into a live troubleshooting bridge. The Commission/PSAP will have access to the Web-based Administrative portal 24x/7x365 to view the ticket and monitor the updates. The fact that call volumes are down significantly is a serious concern. Two processes and tickets are being run in parallel; the first for the failed LNG which is being handled by Tier II Support. Secondly, the NGA 911 local maintenance support will be dispatched to check the POI at the Central Office. If the Commission/PSAP and NGA 911 have an indication of a down LNG, then in fact it is the POI at the Central Office that is at fault and the repair is looked at as soon as access is granted by the incumbent in accordance with SLA's. The other issue is why (a failure at the CO) is presumably impacting Ingress Call Volumes. Since calls are capable of being sent to both CO's even prior to the installation of the ESInet; the transition audit should have identified any OSPs that were not redundantly connected. But as part of the troubleshooting procedure, that is the first place to look; with both Tier II and Tier III support involved and periodic checks back to the Tier I NOC. Between the techs on site and the back office Tier III engineers checking the logs, there is an indication that one of the wireless carriers (MNOs) MSC is not provisioned with a redundant link (or the secondary VLAN they use for connecting to the alternate SR – now LNG, but actually POI is down). The combined support staff knew due to the significant size of calls missed that it had to be a wireless carrier and that is why they looked there first. The MNO contacts their SP and the line is brought back up almost immediately resolving the issue with missed calls. A few hours later the backup POI is repaired (another connectivity issue) and Ingress paths and services are redundant again. However, It is the goal of NGA 911 to avoid a scenario such as the one described. As such, NGA 911 has designed its architecture to include a complete redundant and geographically diverse signaling and call routing/processing systems. All of the NGA 911 SS7 links/systems are quad-versed. The NGA 911 solution has multiple LNG gateways in each of our sites and T1's or DS3's will be distributed over them (example: NGA 911 has 18 in Chi and 4 in St Louis). So a catastrophic LNG gateway failure will cause only a small portion of the traffic to failover. Each LNG gateway has N+1 TDM card redundancy so if a card fails the redundant card will take over. The Gateways themselves are carrier-grade with redundant control, management, processing and power. When connecting with service providers and customers using TDM, we will build 4 connections with 4 trunks. NGA 911 will make sure the LNG gateway				

	resources and TDM transport will be engineered to operate at less than 25% capacity so that even in the unlikely scenario where all LNG gateways in a market are lost, we can provide complete failover between markets. NGA 911 has multiple automated and human-based tools and resources to continuously monitor the TDM, trunks and LNG capacity and resources and kick-off augments when needed.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN SCEN 3	**Scenario 3** As part of normal data-maintenance procedures, the bidder has uploaded six minor recent changes. The bidder's Quality Assurance/Quality Integrity (QA/QI) process provides a discrepancy report detailing 15,000 errors resulting from the updated file.	X			

Bidder Response:

As the Spatial Interface and GIS provider, NGA 911 operates the SI, GIS Services and underlying database and data management.

- **Data Acquisition:** Provisioned data (via upload, SI, or a tool) will be processed via our serverless cloud data pipelining solution.
- **Data Ingestion:** The data pipeline solution will decompose every record and process according to the rules configured. This allows each record to be individually processed by its layer rules. To find the source of the 15,000 errors in the discrepancy report, a definition would be captured and configured as to what layers are being validated in what system, along with what geometry rules are being examined.
- **Data Validation & Augmentation:** The error log would capture the error for each record. Given, the specific records causing the errors would be captured in the processing and the error log would determine each record as to how it is out of standard.
  - **The** relationships built against that record type would be supported in a report as not out of standard as well.
  - **For** instance, a QA/QC discrepancy could occur if all of the mandatory/conditional/optional field validation rules are "turned on", along with the most to least stringent geometry validation rules.
  - If in our system, on this configuration data pipeline generated quality database, rules based on address points and street centerlines are primarily and generally configured to meet the NENA standards as well as regional and state minimum requirements. Errors on individual features loaded (addresses, centerline line segments, etc.) could invalidate other records in a cascade manner as is described.
  - When a validation is performed, all data will be reanalyzed and flagged with any violations. Those will be raised and displayed in the dashboard with the number of geospatial features involved and how much of the total database has this error which we call the error coverage.
- **Data Publishing:** Passing records will move to production, where error records will not be, and records with warning can be determined by governance on how to handle. Also, from a visualization point of view, the ledger and QA/QC database can be queried to support Business Intelligence, Dashboards, and Reporting views.

NGA 911 has a documented functional and technical specification for our

- SI Technical Specification patterned after ATOM replication feed (OGC 10 o69r2, RFC 4287, RF 5023)
- SI Update Specifications supporting bi-directional GIS Updates
- SI Provisioning Data Model (NENA-STA-010.2-2016 (originally 08-003), Appendix B)

	• ECRF LoST Service Interface (RFC 5222) • Discrepancy Reporting [DR] Web Service Interface • Data Pipeline Functional Specification with mapping to NENA standards • Reporting and Dashboard Functional Specification for Address, ALI, GIS, CPE, and CAD query support

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
GEN SCEN 4	**Scenario 4** At 0700, the NOC has received an alarm reporting loss of connectivity for a single path to Host A. At 0705, the NOC contacts Host A to confirm the loss of connectivity. The PSAP has found that the link lights are off, but the system appears to be operational. At 0725, the redundant link appears to be bouncing for Host A. At 0900, the PSAP is reporting a decrease in typical call volume.	X			
	Bidder Response: For this scenario, the indications are that there is an issue with more than Host A, or just an abnormal drop in call volume. For the first indication, all circuits could be down to Host A without impacting calls to the PSAP. Host B ought to be serving the full call volume in this condition. For the design provided by NGA 911, we are ALWAYS aware of the performance of each and every link, connection, and trunk on the network. NGA 911 uses Netflow and sidecars (embedded analysis packets) to continuously track and monitor each for SLA performance KPIs. We NEVER have a single path to a Host facility, with a minimum of two vendor independent fiber links and two public safety grade LTE connections (PSG links are contracted to have Quality, Priority, and Pre-emption). Our Dashboard will indicate immediately any issue with any of the four or more links going to the serving PSAP Host. The NOC will follow up with a call to the PSAPs served by that Host under the terms agreed to by the Commission. - the vast majority will not be service affecting, so we will want to find a level at which we need to make these calls. For the Regions, NGA 911 is delivering traffic to the Host sites and at least in this bid, we have no end to end control into the PSAP. We do RECOMMEND that the Commission consider adding our circuit management capabilities all the way to the PSAP. In that case NGA 911 and the Commission will have a more granular view of the network and connectivity into the individual PSAPs. In the second part of the scenario, if the observed decrease in call volumes is actually due to a fault, this is an indication of a very serious problem where the ESInet and NGCS provider evidently does not have sufficient network management tools to see the impact of the fault at Host A on the overall performance of the end to end service as technically Host B should pick up the call volume and the service provider should be aware of all performance issues in the network at Host A and working to repair them to deliver the service uninhibited. For NGA 911 we track call Ingress by OSP and overtime accumulate AI data related to the expected call volumes. Anomalies here will rise to the attention of the NOC for evaluation. We have already discussed how we track the network and trunks. There is a chance in this scenario, particularly if it is only impacting one PSAP, that the fault rests with the CPE from the Host to the PSAP that the ESInet and NGCS have no oversight of? - Again, we recommend that as part of the ESInet, NGA 911 provide oversight of the link from the Host to the PSAPs.				

Any additional documentation can be inserted here

	Project Management and Ongoing Client Management Services **Project Management Methodology** 1. Describe bidder's project management methodology and support structure. 2. Describe the daily, weekly, and monthly interactions during the migration. 3. Include a proposed high-level project plan. 4. Include a schedule for the through implementation of this project.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
PM 1		X			

Bidder Response:

1. Project Management Methodology:

<u>Approach to Management of Project</u>

Throughout the course of the ESInet and NGCS Project NGA 911 will provide professional services to the State of Nebraska to effectively design and implement the new system as well as smoothly integrate its capabilities into the State's emergency communications processes. These services will be organized around three phases:

Solution Planning. During this phase NGA 911 will collect all the necessary requirements for the project and catalog the needs and constraints of each of the primary and secondary PSAP locations. NGA 911 and the Commission together will agree on the final scope of the project; NGA 911 will document that scope in a master plan which will include a master schedule, a trunk provisioning plan, an OSP aggregation plan, and a PSAP equipment inventory plan and PSAP LAN wiring plan to connect all of the PSAPs to the ESInet.

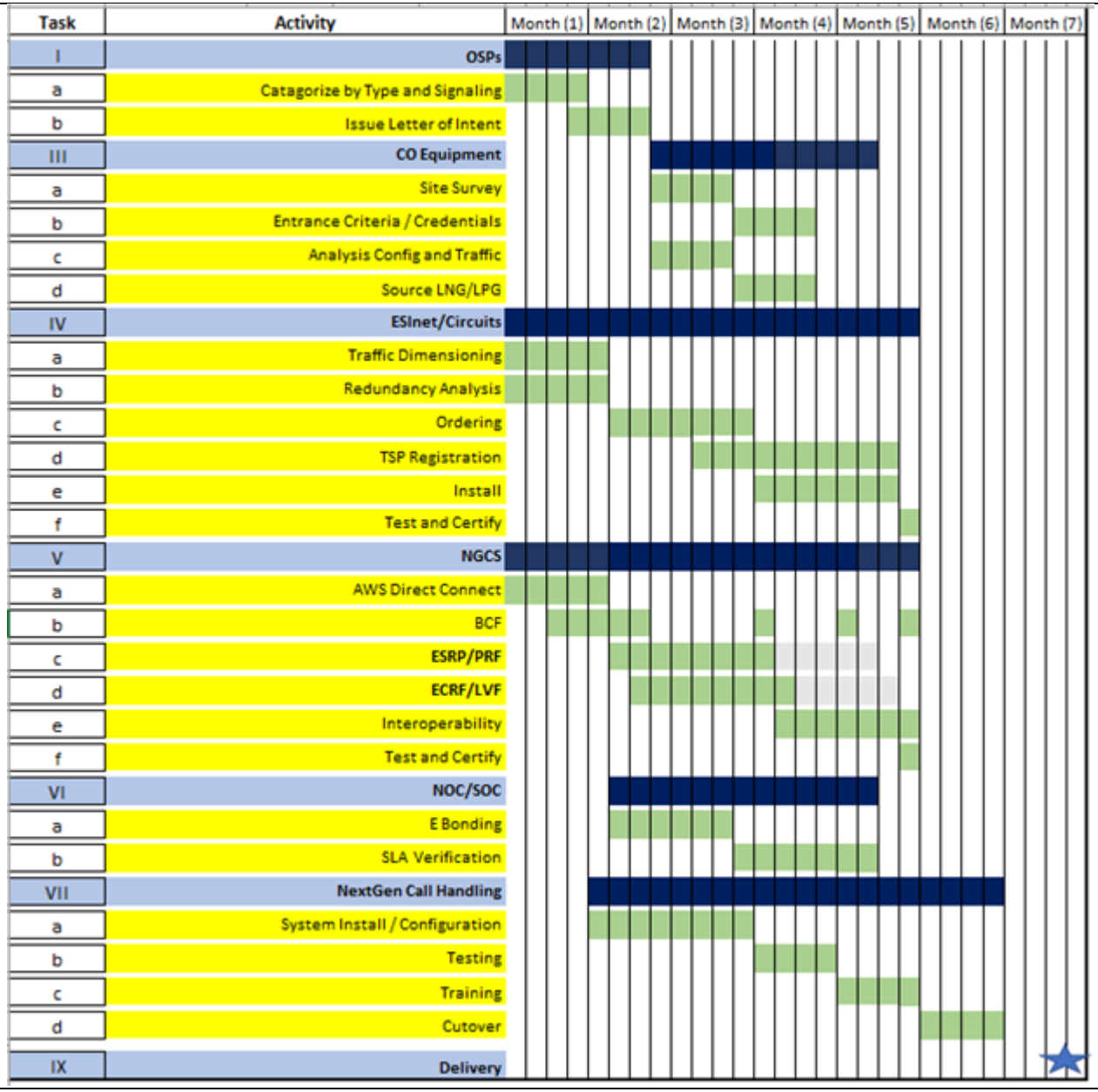
Solution Implementation. In this phase NGA 911 will order, implement, test, validate and accept all the NG trunks required for the PSAPs connections to the NG Core as well as the networking hardware required at the PSAPs to actualize the ESInet and the hardware required to support each of the PSAPs. We will dimension the cloud platform and establish a dedicated instance for the State of Nebraska of the NGCS capabilities. We will implement, test and validate the performance of the OSP interfaces. We will also connect the NOC to all of the solution elements as they are turned and begin monitoring the system.

Solution Testing and Cutover. Once all the solution elements are installed and validated at each PSAP location we will perform rigorous end to end acceptance testing. Once the system passes each of the thresholds in the test plan the system will be ready for cutover and to begin operation. As part of the preparation for going live PSAP personnel will be trained on the new systems during this testing and cutover phase.

All of the services required to complete the tasks listed above will be provided by NGA 911 and reflected as a onetime cost for the initial implementation of our proposed next generation emergency communications system. More details on the cost and timeline for the implementation of these services can be found in the Proposed High-Level Project Plan and Section: Schedule for Life Cycle of the Project. All personnel belonging to NGA 911, who will be working in the State's PSAP locations will be CJIS cleared with the proper documentation submitted to the proper PSAP authority at least 5 days prior to their first visit. NGA 911 understands that all personnel

	must be properly cleared and badged before doing any work in a PSAP and furthermore will abide by any other security requirements that currently exist or may be implemented in the future at any PSAP location in the State of Nebraska. 2. Please see chart below:

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1



	3. A High-Level Proposed Project Plan has been included as an Attachment and labeled according to the RFP requirements. 4. NGA 911 has proven that we can roll out our solution in a well thought out, regional, and phase manner. As we are deploying California Los Angeles and Central Regions we are on track, on budget, and minimal impact to the PSAP. NGA 911 will work with the Commission on an agreed upon plan for the Estimated Regions (subject to change): South Central/Panhandle=Region 1 Southeast 911=Region 2 East Central 911 (including Custer County) = Region 3 Metro=Region 4 North Central=Region 5 Norfolk PD=North East=Region 6 Metro West (anticipated Dodge, Colfax, Cuming, and Burt Counties) = Region 7. After the contract award we will be prepared to start site surveys as soon as the Commission approves our plan and gives approval to start the project. We will have the first PSAP migrated to our solution within 7 months. We will be able to test and turn up to 4 PSAPs a week. A proposed High-Level Project Schedule has been created. The schedule lists the Milestones for the project, along with the steps necessary to complete each of the Milestones listed. The schedule allows NGA 911, as well as the Commission, to monitor the implementation of the project throughout all of the State of Nebraska. NGA 911 will track the major Milestones with the Smart Sheets schedule and the Project Milestone Reports, required by the Nebraska Public Service Commission, State 9-1-1 Department (Commission). Contract start date is to TBD for purposes of sample timeline a start date is assumed.

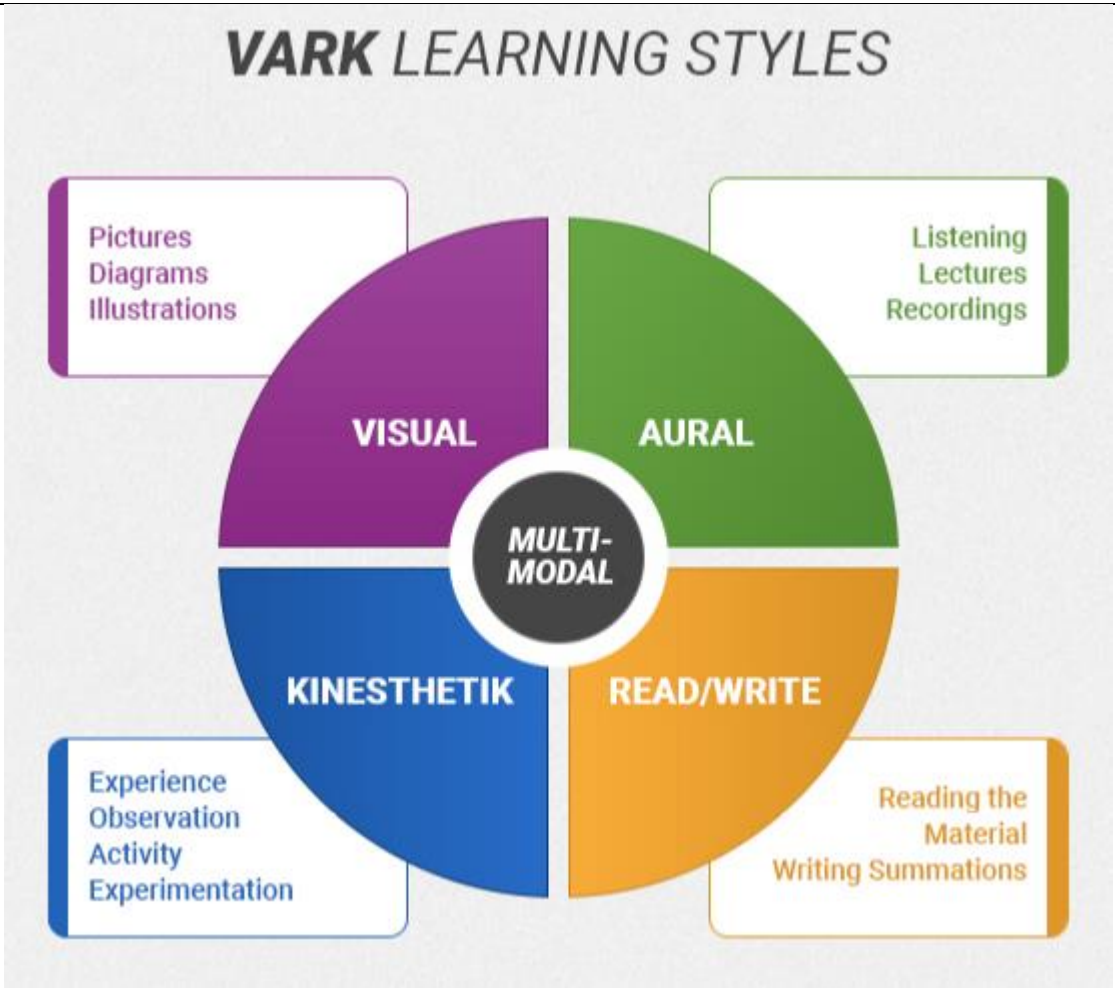
Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
PM 2	**Project Management and Ongoing Client Management Services** **Post-Deployment Client Management** Describe the post-deployment client management service, including client management reports, executive briefings and the fielding of ad hoc support requests.	X			
	Bidder Response: NGA 911 will conduct post-deployment client management calls one (1) week post-deployment, 30 days post-deployment, and then every six (6) months. While these are our pre-scheduled touch points, NGA 911 personnel are available for more frequent status calls or when requested by the PSAP and the Commission. NGA 911 will provide a monthly report, this report will be available through the NGA 911 Web-Portal and will be scheduled for automated delivery based on mutually agreed upon format, i.e. excel, word, pdf, csv on a monthly basis. NGA 911 will work with the Commission on the frequency they would like executive briefings with a minimum of an annual executive briefings face-to-face. NGA 911 will field all ad hoc support requests via our help desk at Support@NGA911.com.				

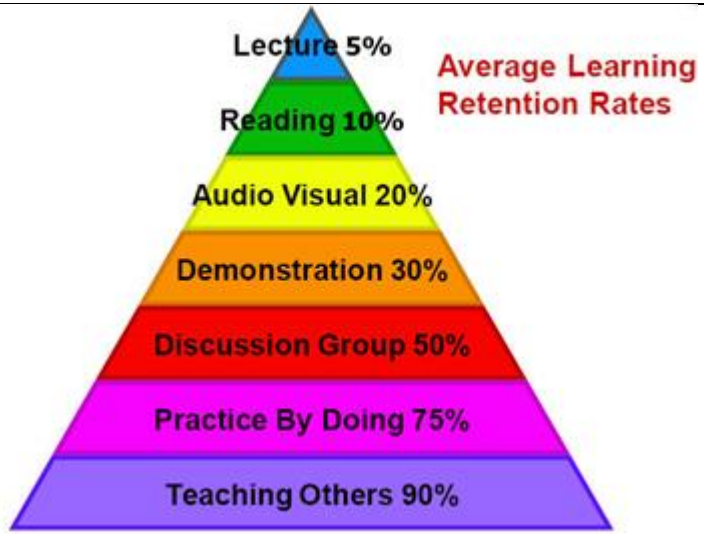
Any additional documentation can be inserted here:

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
TRN 1	**General Requirements – Training** **Comprehensive Training** Contractor shall provide comprehensive training to designated Commission representatives responsible for varying layers of network/system monitoring and system maintenance. Describe bidder's training program for system implementation and ongoing operation and maintenance, including but not limited to the following topics: 1. user-configurable elements; 2. NOC/SOC procedures; 3. escalations; 4. trouble reporting; 5. help desk portal; 6. executive dashboard; and, 7. service monitoring tools. Training shall be available at the user level and delivered to the PSC and each region (up to 10) and also the train-the-trainer level (up to 25 individuals).	X			
	Bidder Response: NGA 911 is a customer-oriented organization that takes a systematic approach to Training. Our courses take into account the four (4) perceptual modalities (preferred learning styles): Visual, Aural, Read/Write, and Kinesthetic. NGA 911 has engineered courses that will engage the adult learner on as many of these styles as possible during each course. To ensure maximum retention of the adult learner we have incorporated the following teaching tools: **Visual Learners** – we provide charts, graphics, and pictures making the training highly visual with screen shots to show the relationships between the tools and the material. **Auditory Learners** – we provide the training verbally as they per to hear rather than reading or seeing the material displayed visually. **Reading/Writing Learners** – we provide annotated handouts of the presentation so they can read along and provide the chance to write down what they have learned. **Kinesthetic Learners** – we provide hands-on experience with our training mode of the Web-based portal to practice what they are learning.				



By incorporating these teaching tools, we know that the adult learner's retention rate is increased to 75%.



Attendees are encouraged to ask questions during the sessions for maximum retention. NGA 911's training program for system implementation and ongoing operation and maintenance, will including but not limited to the following topics:

1. User-configurable elements
2. NOC/SOC procedures
3. Escalations
4. Trouble reporting/ help desk ticketing/escalation
5. Help desk portal/web-based portal
6. Executive dashboard
7. Service monitoring tools/dashboards
8. Reports/canned/ad-hoc
9. Network monitoring
10. High level GIS data entry
11. Online Resources
12. Training Manuals/raining Videos
13. Disaster Recovery
14. NIMS
15. Review/Questions and Answer

	NGA 911 will conduct training in-person, via tele-conference, and provide pre-recorded tutorials that can access 24x7x365 at their convenience. **SESSION ONE - 2 HOUR WEB BASED TRAINING CURRICULUM:** · Web User Trouble Reporting Interface Overview · Network/Monitoring/Help Desk Web Interface · Service Monitoring Tools · Trouble Reporting · Help Desk 877-899-8337 press #2 **SESSION TWO - 1 HOUR WEB BASED TRAINING CURRICULUM:** · Next Generation Core Services · ESInet · Policy Routing Function (PRF) · Legacy Network Gateway (LNG) · Border Controller Function (BCF) · Emergency Service Routing Proxy (ESRP) · Emergency Call Routing Function both Legacy and NG9-1-1

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
TRN 2	**General Requirements – Training Attendees and Curriculum** 1. Describe the number and types of attendees required to attend training, training curriculum, number of training attendees included in the proposed price, and the duration of the training program per attendee (expressed in hours per day and number of days), as well as the location of the training and whether such training is available online or onsite. Preference is given to training that can be conducted in an onsite setting for attendees. 2. Provide Examples of the proposed training plans. 3. Provide a sample of the training materials to be used. Training classes shall be recorded for future reference and training of new Commission and PSAP employees.	X			
	Bidder Response: 1. NGA 911 will adhere to the state and local guidelines for public gathering limitations and conduct training for the allowed amount of attendees. NGA 911 will have the following types of training: • Admin • Train the Trainer • End User NGA 911 training curriculum will cover: • User-configurable elements • NOC/SOC procedures • Escalations • Trouble reporting/ help desk ticketing/escalation • Help desk portal/web-based portal • Executive dashboard • Service monitoring tools/dashboards • Reports/canned/ad-hoc • Network monitoring • High level GIS data entry • Online Resources • Training Manuals/raining Videos • Disaster Recovery • NIMS • Review/Questions and Answer NGA 911 will conduct training in-person, via tele-conference, and provide pre-recorded tutorials that can access 24x7x365 at their convenience. NGA 911 will train all personnel that will be utilizing the system.				

	The duration of training is: • Admin - 1 day for 3 hours • Train the Trainer - 1 day for 3 hours • End User - 1 day for 2 hours NGA 911 will conduct training onsite at an agreed upon location to accommodate the State imposed restrictions on gatherings. 2. NGA 911 has provided Examples of the proposed training plan as an attachment and labeled as required by the RFP. 3. NGA 911 sample training materials are included in the Example Training Plans. Training classes will be recorded for future reference and training of new Commission and PSAP employees.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SRAR 1	**General Requirements – Service, Repair and Advance Replacement** The Commission shall not be responsible for the replacement and maintenance of hardware and software required to provide the NGCS or ESInet connectivity provided as part of the bidder's solution. The Contractor shall resolve all faults or malfunctions at no additional cost to the Commission. **Support Maintenance** 1. Describe in detail bidder's 24 x 7 x 365 maintenance support for the life of the contract. 2. Describe bidder's understanding of public safety maintenance windows and associated notification processes. 3. Describe bidder's problem resolution and change management processes, the supporting systems, and adherence to best practices, such as those described in the ITIL version 3 or most current version.	X			

Bidder Response:

1. The NGA 911 proposed solution is a redundant and fully managed service that includes 24x7x365 Help Desk, Maintenance Support, NOC/SOC, training/continued training, and Dashboard MIS including Ad Hoc reporting for the life of the contract. NGA 911 has a secure 24x7x365 Administrative Web-based portal for help desk and technical services support. The Commission or PSAP can obtain information, updates, and status of service issues, account information, including but not limited to help with the reporting system.

The Commission or PSAP may request assistance or report trouble in three ways:

1. By dialing 1-877-899-8337; Option 2 and report trouble directly to the Help Desk
2. By sending an email to Support@NGA911.com
3. via Web Portal by accessing the Incident Management System (IMS) via the NGA 911 Dashboard

NGA 911 will provide 24x7x365 maintenance support for the life of the service-based solution. NGA 911 customers will receive Help Desk and technical services support for all products and services included in NGA 911's proposed solution.

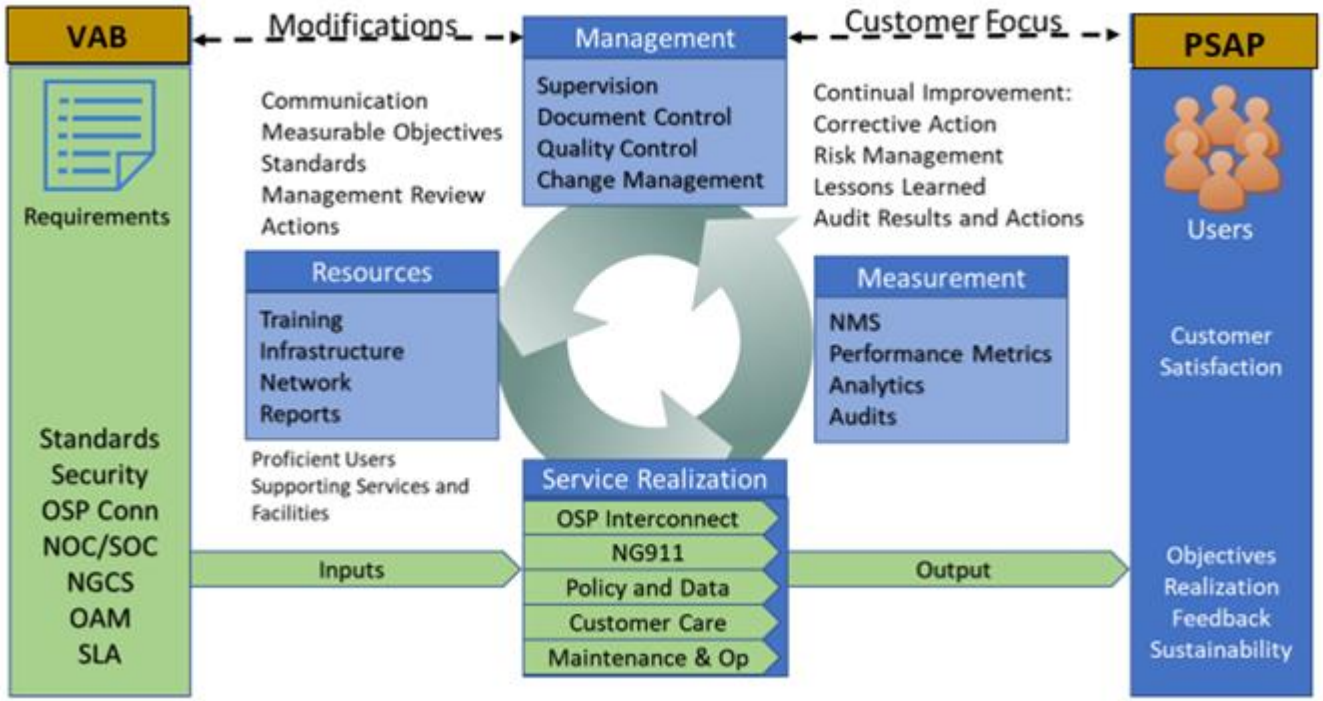
In addition to service response and service resolution, the escalation matrix helps ensure available resources are focused on problems that severely affect service. This table defines when additional resources are notified to ensure management is aware of problems and can provide troubleshooting support.

2. NGA 911 understands the Public Safety Maintenance windows and associated notification processes. NGA 911 will perform necessary maintenance during the standard Public Safety Maintenance Window of midnight - 4:00 A.M. Monday - Thursday. However, NGA 911 will work with the Commission and PSAP to pre-define the Public Safety Maintenance Window if the standard NGA 911 Public Safety Maintenance Window is not conducive to PSAP operations.

	The NGA 911 procedure for any maintenance for hardware/software upgrade and/or replacement is as follows: NGA 911 will provide release notes to the Commission and PSAP a minimum of 45 days before implementation. This documentation details the deployment process and timeline for scheduled and maintenance releases. Also, a description of how releases shall be tested within the ESInet and/or NGCS. As a standard, maintenance and service events are planned for Monday through Thursday between the hours of midnight - 4 A.M. local time. However, NGA 911 will work with the State of Nebraska PSAPs to define the Public Safety Maintenance Window that is most appropriate for them – based on PSAP operations. NGA 911 will work with the State of Nebraska to review the following types of information to determine the most appropriate scheduling for all serviceable events. The types of information include: • Busy hour calculations • Busy day calculations • Local planned and special events • Local planned Police Department and Sheriff's Office events • PSAP resources • Weather NGA 911 Operations Staff will make advance notification of planned maintenance work to the State of Nebraska PSAPs. Notification will depend on the event type and will occur a minimum of 7 days in advance for all core hardware replacement events and a minimum of 48 hours in advance for all general serviceable events. Notification will occur via email and other formats, as agreed. NGA 911 Operations Staff will confirm receipt of notification and approval of the day and time for the event in advance. In addition, prior to initiation of any event, State of Nebraska/PSAP personnel will be requested to confirm that call volume is acceptable for a serviceable event and that there are no critical issues under management at that time. Should the serviceable event be critical in nature, the initiation time will be managed with the State of Nebraska/PSAP to ensure resolution of the critical issue in a timely manner. 3. Conformance with Best Practices for Service Delivery Management As part of our overall Service Delivery Management System (QMS), NGA 911 incorporates the Information Technology Infrastructure Library (ITIL) version 3 service for problem and change management methods and procedures during the initial implementation and ongoing operations of the State's NGCS and/or ESInet.

NGA 911 adheres to the eight quality management principles: customer focus, leadership, employee involvement, process approach, system approach to management, continual improvement, factual approach to decision making and mutually beneficial supplier relationships.

A continual improvement processes will be integrated throughout the program, from commencement to ongoing operations, to assure compliance with requirements, fulfilment of contract performance standards and the delivery of increasing customer satisfaction.



The focal point of our processes is Service Realization in the form of delivering, operating, and maintaining the NGCS and ESInet to the highest possible standards; and continual improvement of services and capabilities for the direct benefit and to the satisfaction of the customer - the first responder community. Keys elements to achieving these goals are, amongst others: (1) meeting State

	objectives, (2) a responsive and effective customer care focused approach, (3) consistent maintenance and operations to include continual enhancement of features and capabilities, and (5) a sustainable business model for the State. Service Realization performance, as the focal point of the program, is directly monitored through the quality assurance reporting elements covering critical performance aspects of the contract to achieve the following requirements: (1) demonstrate conformity to the City's requirements, (2) ensure conformity to Service Realization requirements, and (3) continually improve the effectiveness of the process and our performance results. Our Management processes drive commitment to continual improvement and effectiveness by: (1) communicating to Partners the importance of meeting contract and statutory requirements, (2) ensuring measurable quality objectives are established, (3) conducting management reviews with meaningful actions, and (4) ensuring the availability of resources to implement an effective Change/Service Management Process. Our Resource Management processes provide for the training and sustainment of the required number of proficient and committed personnel with the requisite qualifications and certifications, and the facilities, infrastructure and work environments to enable personnel to deliver quality maintenance, continually improve services, and enhance customer satisfaction by meeting or exceeding customer requirements.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SRP 1	**General Requirements – Software Release Policy** **Scheduled Releases** **Frequency of Scheduled Releases** 1. Describe the frequency of scheduled software releases, the feature release testing process, and the decision-making processes involved in deciding what features and defect resolutions to include in a scheduled release. 2. Include a current roadmap of feature updates and additions with projected release by quarter and year.	X			

Bidder Response:

1. The frequency of scheduled software releases depends on the systems involved. Operating System Software of Standards based functional elements are not subject to change except for the rare case of a bug or to fix performance issues. Standards have been adopted and tested with both CPE Vendors and OSPs. Any changes to the Operational System could have significant impacts on those interfaces. The Portal, reporting systems and other features, services, and functions that either are not defined in the standard and have no direct impact on operations are permitted to be customized.

Features, services, and functions that are enhancements to the standard operation are subject to changes and adjustments much more regularly. The feature release testing process, and the decision-making processes are invoked when deciding what features and defect resolutions to include in a scheduled release. NGA 911 will make documentation of release notes available to the Commission a minimum of 45 days before implementation. This documentation details the deployment process and timeline for scheduled and maintenance releases. A description of how releases shall be tested within the ESInet, including call handling equipment is included in this documentation.

2. NGA 911's current roadmap of feature updates and additions includes proactively maintaining all security patches and related software and firmware updates for the system, including any third-party components. NGA 911 will ensure software updates are performed within 15 calendar days of test lab validation.

NGA 911 proactively replaces any hardware and software that has reached EOS or is defective or unserviceable due to failure or malfunction. NGA 911 is a managed service solution and will perform this service at no additional cost to the Commission or PSAP.

Our patch management solution administers software updates for system nodes, giving our Security Operations Center (SOC) the ability to view installed software revisions and determine what security patches need updating in order to maintain optimal security. In addition, our solution includes a threat exposure (vulnerability) assessment capability that collects data and analyzes risk in the environment. Application and operating system/firmware patches are distributed without disruption to the NGCS itself. Since nodes are virtualized within the NGCS and run in an active-active configuration, specific nodes can be taken out of service to allow for the installation of patches and subsequently be returned to service, all without affecting service availability. This maximizes both the

	availability and the security posture of the NGCS. We manage these patches and updates through our rigorous DevOps and Change Management process. Projected release by quarter and year: As soon as it is discovered a patch is required, the patch goes in our lab. NGA 911 will ensure software updates are performed within 15 calendar days of test lab validation. **Release Types are defined as follows below:**

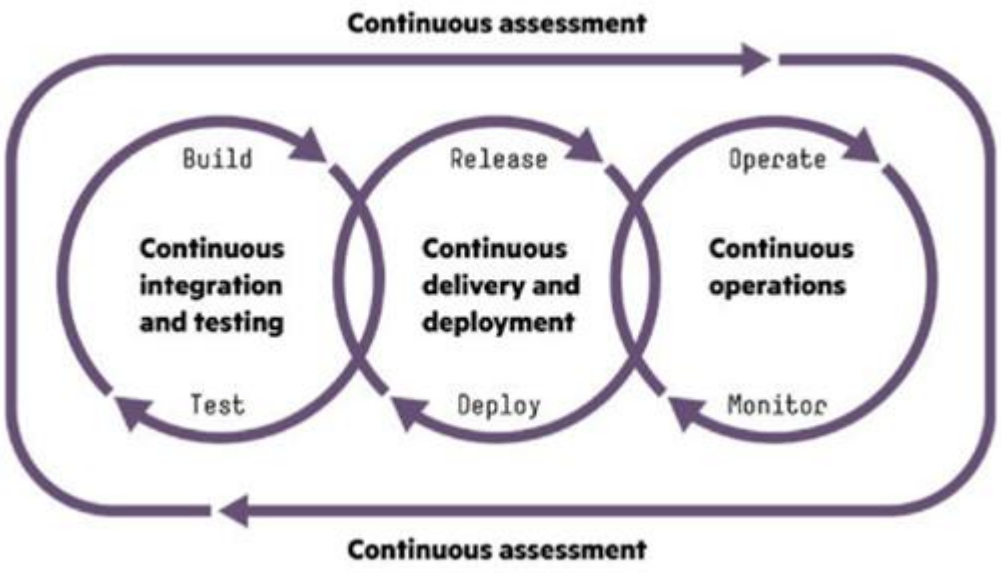
Any additional documentation can be inserted here:

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

Major Release Semi Annually	• Major new features, architecture changes, product components • Full, standalone product build • Will normally be localized • Naming convention: X.0
Minor Release Quarterly	• Significant new features beyond previous minor/major version • Full, standalone product build • Will normally be localized • Naming convention: X.Y
Maintenance Release As needed	• May include previously released Service Packs and other fixes • Full, standalone product build • Naming convention: X.Y.Z
Service Pack As needed	• Periodic rollup of Hot fixes and Patches • May only be a set of files, not a full, standalone product build • Released on a planned availability date • Recommended to all customers as part of a proactive maintenance plan • Will not normally be localized • Naming convention: X.Y Service Pack #Z
Patch As needed	• In response to a specific Software Failure • May only be a set of files, not a full, standalone product build • Released ad-hoc, as soon as available • Recommended to all customers to prevent a critical failure • Will not normally be localized • Naming convention: X.Y Patch #Z
Hotfix As needed	• In response to a specific customer-reported Software Failure • May only be a set of files, not a full, standalone product build • Released ad-hoc, as soon as available, via Tech Support only • Typically created in response to Severity-1 issues from Premium Support customers • Will not normally be localized • Naming convention: X.Y Hotfix #Z

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

	General Requirements – Software Release Policy **Maintenance Releases** Describe the frequency of defect-resolution software releases, as well as the decision-making processes involved in selecting which software defects to fix.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
SRP 2	Bidder Response: NGA 911 ESInet is a cloud-based solution therefore the Commission will not be responsible for replacement of hardware and software for the ESInet and the NGCS. Cloud computing has the servers off-premise. NGA 911 takes care of them for you and will install regular software updates – including security updates ensuring your PSAP operates on the updated and tested software releases. During the life of the contract, NGA 911 will maintain and monitor all equipment and software within the NGCS solution. **The Decision Making Process** In order to maintain optimal router, switch, and functional element configurations, NGA 911 adheres to the continuous assessment model depicted in the diagram below. Build types are characterized as being based on Customer Needs, on Enhancements, and on Operational Necessity. Each type is coded in an Agile manner and integrated into the Test Environment. After successful testing, the releases are delivered in the parallel active-active manner described above. Utilizing the capabilities of our NOC/SOC software defined WAN; direct and immediate comparisons are made between the new load and current release. Performance is verified on a number of metrics including end-to-end jitter, latency, MOS fidelity, and call response times for both. Any findings or measurements that fall out of the specified norm for the new release result in an automatic restoration to the current release.				



Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SRP 3	**General Requirements – Software Release Policy** **Test Environment** Prior to install of new releases, bidder shall explain how Contractor replicates the production environment for software release testing to provide assurances that future software releases will not negatively impact PSAP operations.	X			

Bidder Response:

Pre-production Testing Environment

New functions and features are subject to thorough and robust testing in a pre-production environment. When code is ready for deployment the release process is structured to maintain the current load for a fixed period of time.

NGA 911 utilizes the CI/CD method of software development. Each software feature, fix or update follows strict guidelines and rigorous standards prior to any deployment into a production environment. Creating code starts at the local level from the development team. The code must first pass testing and optimization locally before the code can be pushed to the environment. Once the code enters the second stage of the process the code is then scrutinized, reviewed, tested and optimized once again by a team of developers. Updates and changes are cataloged before the code is moved to the next level.

The code is then moved to the staging environment. At this level of the development the software code is then reviewed and tested by the senior development team in an environment that mimics the production environment to ensure that all bugs have been captured, recorded and fixed prior to being deployed into the production environment. When the development team is ready to deploy the project manager will contact the customer to schedule a maintenance window for deployment. During that window the development team will remain on standby while the code is being deployed. It takes approximately 15 minutes for the updated code to be deployed throughout all of the instances and availability zones. NGA 911 will maintain the original coding in a separate branch in the event that there is a need to revert back to the previous version of software.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
SRP 4	**General Requirements – Software Release Policy** **Access to Defect Tracking System** Contractor shall provide the Commission with access to the Contractor's defect tracking system for the Commission to track the progress of defect resolutions. **Software Defect Tracking Process** Provide a detailed description of the software defect tracking process and describe how bidder will provide training for no more than ten (10) people to Commission staff prior to Final Acceptance Testing.	X			

Bidder Response:

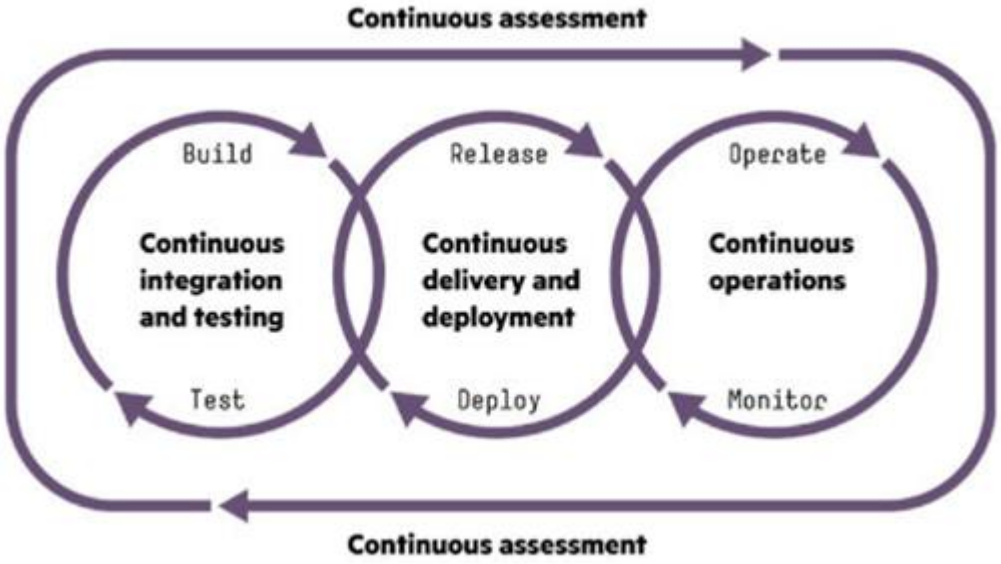
Access to Defect Tracking System

NGA 911 will provide the Commission and PSAP with access to the defect tracking system in order for the Commission and PSAP to track the progress of defect resolutions through the NGA 911 web-based Incident Management System (IMS) (defect tracking system).

The IMS generates an incident that remains open and in queue until it is resolved. The NGA 911 IMS allows for incident management capabilities for trouble ticket management. It keeps a log of troubleshooting and/or research performed. The Self-Service Portal is available 24x7x365 which gives the customer greater reach and flexibility. The Commission and PSAP can submit and check the status of incidents, view notes and history. Once a Commission or PSAP member notifies NGA 911 of an issue, they will be provided a unique incident number, date and time opened, status of the ticket, and description of the problem reported via email, if available, or by voice. All notes regarding troubleshooting and/or research performed are documented in the notes field and are readily available to the customer. Each incident is assigned a priority level and updates or changes to the priority level are automatically entered in the tracking log with the user ID of the individual making the change along with a timestamp. Additionally, the NGA 911 Trouble Ticketing System allows the customer to pull their reports of open and closed incidents.

NGA 911's IMS automatically sends email updates to the Commission and PSAP members whenever a change is made to the incident including all notes made to the tracking log, priority level changes, and incident closure. Additionally, a Technical Service Representative will be assigned to monitor, and notify the Commission and PSAP member via telephone with updates.

In order to maintain optimal router, switch, and functional element configurations, NGA 911 adheres to the continuous assessment model depicted in the diagram above. Build types are characterized as being based on Customer Needs, on Enhancements, and on Operational Necessity. Each type is coded in an Agile manner and integrated into the Test Environment. After successful testing, the releases are delivered in the parallel active-active manner described above. Utilizing the capabilities of our NOC/SOC software defined WAN; direct and immediate comparisons are made between the new load and current release. Performance is verified on a number of metrics including end-to-end jitter, latency, MOS fidelity, and call response times for both. Any findings or measurements that fall out of the specified norm for the new release result in an automatic restoration to the current release.



Software Defect Tracking Process

NGA 911's Security Scanning is standard part of our Security Operations Center KPI's. In adherence with our defense in depth security framework; we conduct regular tests and scans on our systems, processes and procedures both internally and through third party audits. Additionally, we utilize artificial intelligence (AI) to continuously scan and identify vulnerabilities in the network and software.

As part of the Service and Maintenance included with our contract, we will provide the State with rights to conduct vulnerability scans during prescribed hours and under certain conditions of notification (to protect the SOC and/or NOC from inadvertently overreacting to beneficial scans): Such scans are to be conducted with the intent of:

- An analysis of internal and external technical and security vulnerabilities
  - Common mistakes and configuration weaknesses
  - To ensure business sensitive information is hardened.
  - Check for missing patches: Patch management.
  - Application Bugs: Avoiding cyber security breaches
  - Attack surface reduction: finding exposures that may not be necessary, and removing them to avoid future problems.
  - Encryption weaknesses: finding and resolving any weaknesses in algorithms.

	• Evaluation of passwords, logins, and security policies • Verifying Network Security Reports • Checking and verifying network access and performance security NGA 911 will provide training for no more than ten (10) Commission staff prior to Final Acceptance Testing.

Any additional documentation can be inserted here:

SRP 5	**General Requirements – Software Release Policy** **Software Defect Aging** Describe how service-affecting software defects are aged. If minor problems (from the Contractor's perspective) are not identified and resolved immediately, these minor problems can become major or critical problems. Describe in detail how/when this minor problem gets scheduled or automatically escalated, and the feedback mechanism in place for keeping the Commission informed.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: NGA 911 uses Bitbucket from Atlassian to manage defects and defect aging. Bitbucket is a web-based version control repository hosting service owned by Atlassian, which we use for source code and development projects that use our Git revision control systems. We have daily scrum meetings where we review all the active items in Bitbucket. These are broken into two major categories. Operational Software and Service based software. This division ensures that operational affecting software is top and center in the daily, weekly, and monthly sprints; so that minor issues do not rise up to become more significant and are dealt with early. See chart below for timelines.				

Any additional documentation can be inserted here:

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

Major Release Semi Annually	• Major new features, architecture changes, product components • Full, standalone product build • Will normally be localized • Naming convention: X.0
Minor Release Quarterly	• Significant new features beyond previous minor/major version • Full, standalone product build • Will normally be localized • Naming convention: X.Y
Maintenance Release As needed	• May include previously released Service Packs and other fixes • Full, standalone product build • Naming convention: X.Y.Z
Service Pack As needed	• Periodic rollup of Hot fixes and Patches • May only be a set of files, not a full, standalone product build • Released on a planned availability date • Recommended to all customers as part of a proactive maintenance plan • Will not normally be localized • Naming convention: X.Y Service Pack #Z
Patch As needed	• In response to a specific Software Failure • May only be a set of files, not a full, standalone product build • Released ad-hoc, as soon as available • Recommended to all customers to prevent a critical failure • Will not normally be localized • Naming convention: X.Y Patch #Z
Hotfix As needed	• In response to a specific customer-reported Software Failure • May only be a set of files, not a full, standalone product build • Released ad-hoc, as soon as available, via Tech Support only • Typically created in response to Severity-1 issues from Premium Support customers • Will not normally be localized • Naming convention: X.Y Hotfix #Z

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
DOC 1	**General Requirements – Documentation** The Contractor shall provide the Commission with all pertinent documentation for the ESInet and/or NGCS connectivity provided as part of the Contractor's solution as implemented, No more than 30 days after completion of the network construction, and update the Commission as configurations change over the term of the contract. The required documentation shall include the following: **1.** Detailed project plan; **2.** Escalation procedures; **3.** Circuit identification; **4.** Single points of failure; **5.** Network path diversity drawings into each PSAP; **6.** Network path diversity drawings into each non-PSAP site or structure housing any element or device that is part of the overall system; **7.** PSAP backroom as-built drawings; **8.** PSAP demarcation point drawings; and, **9.** All user interface training and reference materials. **Network As-Built Documentation** Upon implementation, Contractor shall provide a network or solution diagram that clearly depicts the Contractor's solution as implemented. The Contractor shall provide all documentation in agreed-upon electronic format via a Contractor-hosted web portal. Please describe how bidder's solution meets or exceeds this requirement.	X			
	Bidder Response: NGA 911 will provide the Commission all pertinent documentation for the ESInet and/or NGCS connectivity we are providing as part of the NGA 911's solution as implemented. NGA 911 will supply the documentation no more than 30 days after completion of the network construction. NGA 911 will update the Commission if configurations change over the term of the contract. NGA 911 will provide the following: 1. Detailed project plan; 2. Escalation procedures; 3. Circuit identification; 4. Single points of failure; 5. Network path diversity drawings into each PSAP; 6. Network path diversity drawings into each non-PSAP site or structure housing any element or device that is part of the overall system; 7. PSAP backroom as-built drawings; 8. PSAP demarcation point drawings; and, 9. All user interface training and reference materials.				

	Network As-Built Documentation Upon implementation, NGA 911 will provide the Commission a network or solution diagram that clearly depicts NGA 911's solution as implemented. NGA 911 will provide all documentation in an agreed-upon electronic format via a NGA 911 hosted web-based portal. All plans, training, manuals, reports, and analytics will be readily accessible in our web-based portal for access 24x7x365.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 1	**Next Generation Core Services Elements (NGCS)** Provide a network or solution diagram that clearly depicts the bidder's proposed transitional and end state for the Commission's ESInet and NGCS, taking into account the hosts and PSAPs listed in Attachment A - PSAP Host End-Point Locations. The following functional elements and services shall be included: a. Originating Service Provider (OSP) Connectivity; b. Legacy Network Gateway (LNG); c. Border Control Function (BCF); d. Emergency Services Routing Proxy (ESRP); e. Policy Routing Function (PRF); f. Emergency Call Routing Function (ECRF); g. Location Validation Function (LVF); h. Spatial Interface (SI); i. Location Database (LDB); j. Discrepancy Reporting; k. Logging and Recording; l. Time Server; m. Alarm Integration; and, n Message Session Relay Protocol (MSRP). **Originating Service Provider (OSP) Connectivity** **Due Authorization** Bidder shall possess a certificate of public necessity to operate as a telecommunications provider in the state of Nebraska. The Contractor shall provide a copy of current certificate of public necessity prior to award of contract. **Identification of Service Providers Connected to the Legacy Selective Router** Contractor shall be responsible for identifying and for connecting all wireline, wireless, Voice over IP (VoIP), telematics, and other third-party service providers currently connected to the existing legacy selective router. Contractor shall be responsible for updating this information quarterly for the term of the contract. Bidder shall identify each service provider that will be utilized by Contractor.	X			
	Bidder Response The NGA 911 solution as depicted in the diagrams below is compliant with NENA i3 and all the transitional elements necessary to deliver an i3 SIP INVITE to the BCF. The solution also provides for an LSRG to transfer calls out to non i3/SIP PSAPs through their Selective Routers. Figure 1 Overall NGCS with Legacy, Network, Management, and most Functional Elements				

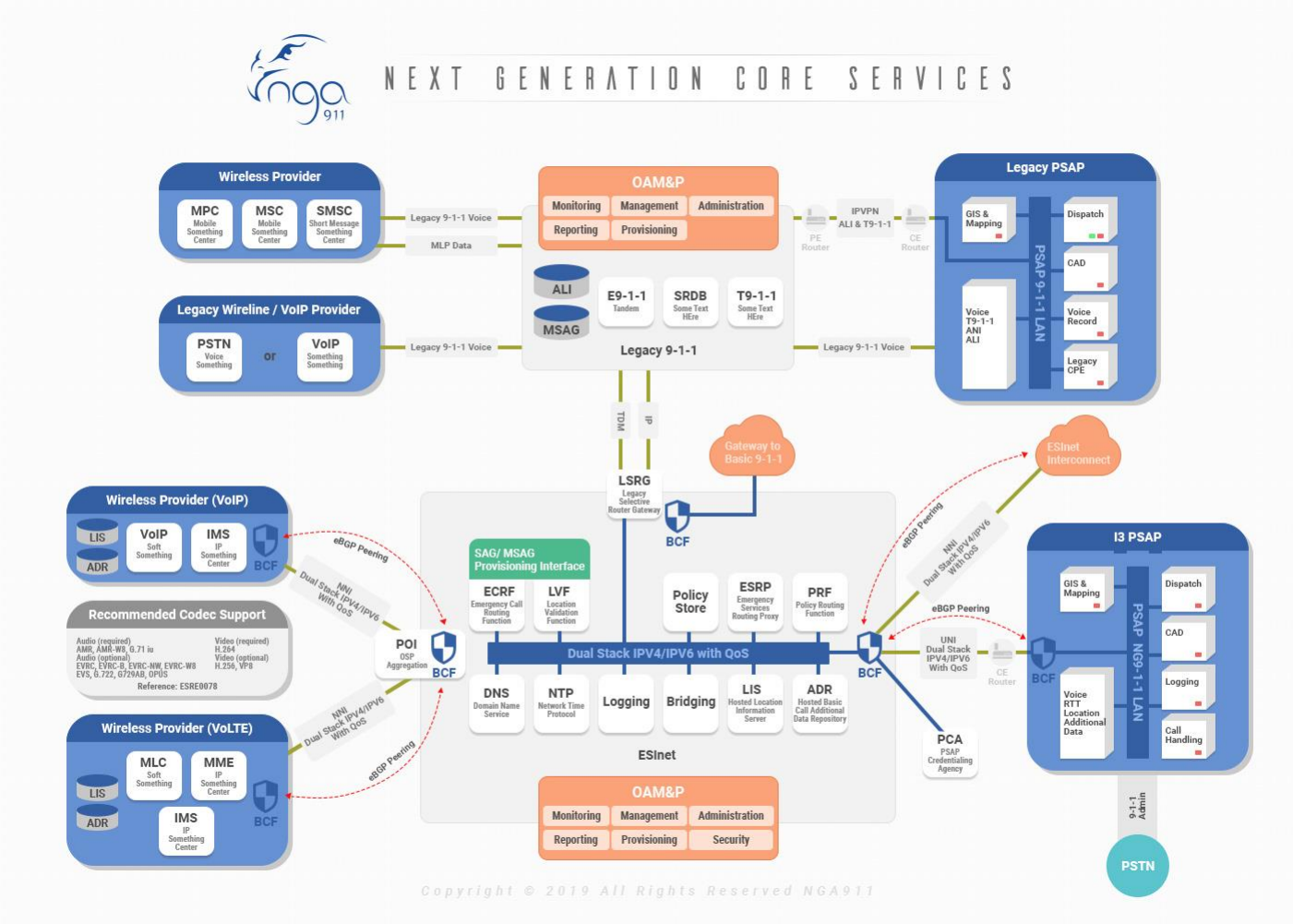
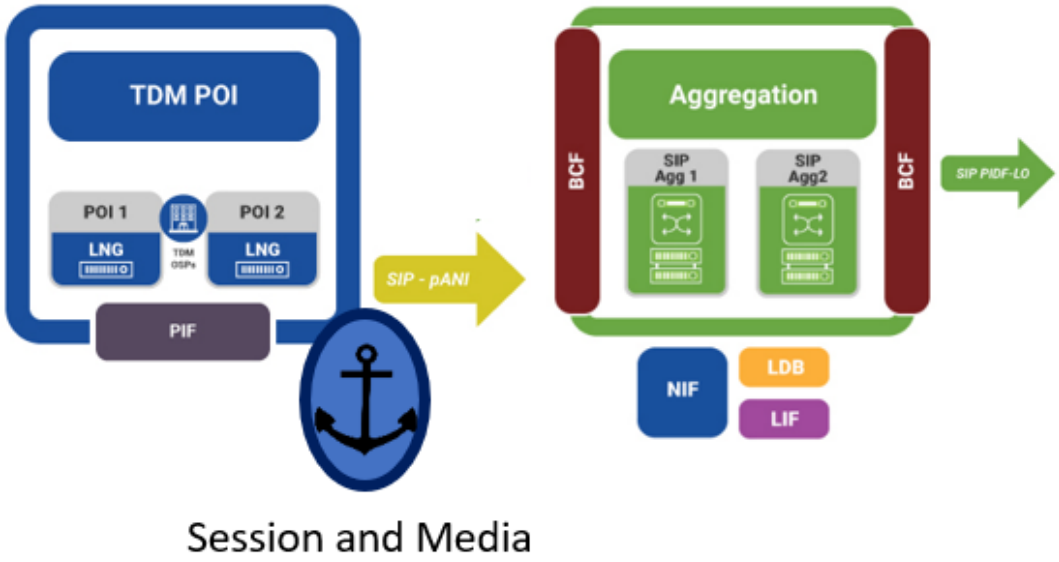

NEXT GENERATION CORE SERVICES
Wireless Provider
MPC Mobile Something Center
MSC Mobile Something Center
SMSC Short Message Something Center
Legacy 9-1-1 Voice
MLP Data
Legacy Wireline / VoIP Provider
PSTN Voice Something
or
VoIP Something Something
Legacy 9-1-1 Voice
OAM&P
Monitoring
Management
Administration
Reporting
Provisioning
ALI
MSAG
E9-1-1 Tandem
SRDB Some Text HEre
T9-1-1 Some Text HEre
Legacy 9-1-1
PE Router
IPVPN ALI & T9-1-1
CE Router
Legacy 9-1-1 Voice
Legacy PSAP
GIS & Mapping
Dispatch
CAD
Voice T9-1-1 ANI ALI
Voice Record
Legacy CPE
PSAP 9-1-1 LAN
TDM
IP
LSRG Legacy Selective Router Gateway
BCF
Gateway to Basic 9-1-1
ESInet Interconnect
Wireless Provider (VoIP)
LIS
ADR
VoIP Soft Something
IMS IP Something Center
BCF
eBGP Peering
NNI Dual Stack IPV4/IPV6 With QoS
Recommended Codec Support
Audio (required) AMR, AMR-W8, G.71 iu
Audio (optional) EVRC, EVRC-B, EVRC-NW, EVRC-W8 EVS, G.722, G729AB, OPUS
Video (required) H.264
Video (optional) H.256, VP8
Reference: ESRE0078
POI OSP Aggregation
BCF
NNI Dual Stack IPV4/IPV6 With QoS
eBGP Peering
Wireless Provider (VoLTE)
LIS
ADR
MLC Soft Something
MME IP Something Center
IMS IP Something Center
BCF
SAG/ MSAG Provisioning Interface
ECRF Emergency Call Routing Function
LVF Location Validation Function
Policy Store
ESRP Emergency Services Routing Proxy
PRF Policy Routing Function
Dual Stack IPV4/IPV6 with QoS
DNS Domain Name Service
NTP Network Time Protocol
Logging
Bridging
LIS Hosted Location Information Server
ADR Hosted Basic Call Additional Data Repository
ESInet
OAM&P
Monitoring
Management
Administration
Reporting
Provisioning
Security
BCF
eBGP Peering
NNI Dual Stack IPV4/IPV6 With QoS
eBGP Peering
UNI Dual Stack IPV4/IPV6 With QoS
CE Router
PCA PSAP Credentialing Agency
BCF
I3 PSAP
GIS & Mapping
Dispatch
CAD
Voice RTT Location Additional Data
Logging
Call Handling
PSAP NG9-1-1 LAN
9-1-1 Admin
PSTN
Copyright © 2019 All Rights Reserved NGA911

Figure 2 The LNG Function at the TDM (PIF) and SIP Aggregation (LIF and NIF) – with LDB – MPC example



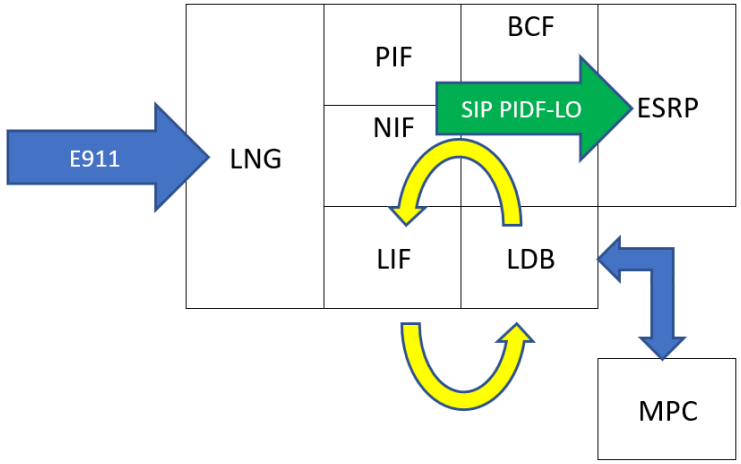


Figure 3 An example BCF – in this case for the OSP. – others defined for ESInet, PSAP/Host, NMS/MIS, and Dashboard in BCF section

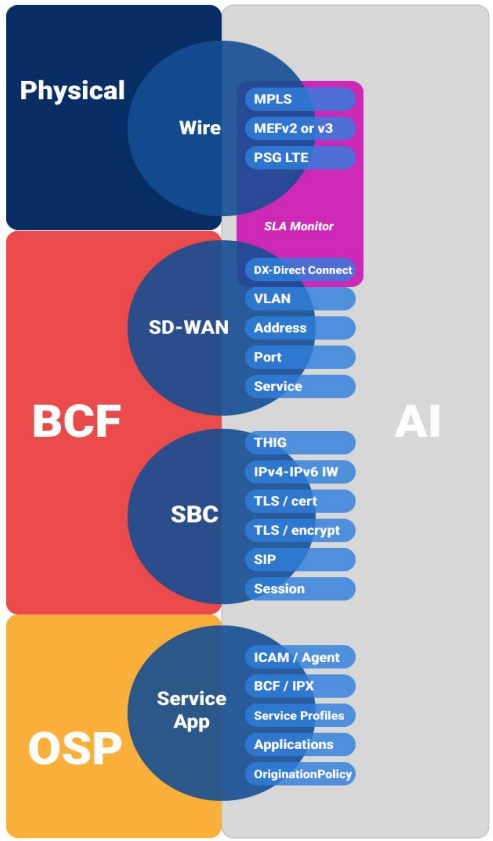


Figure 4 The NGCS to include the ESRP, PRF, ECRF, LVF – and LDB for transition.

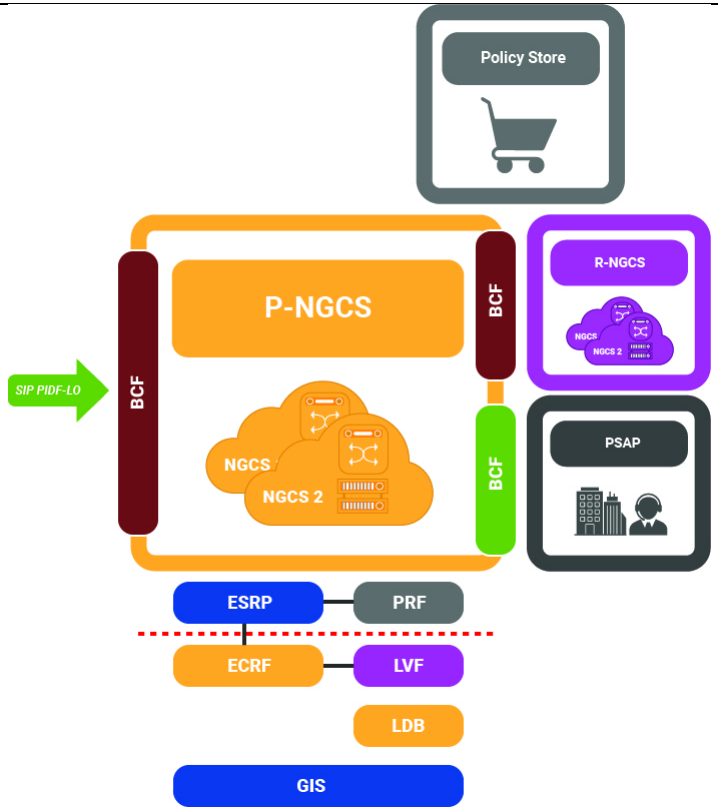


Figure 5 – The SI and QA/QC Process

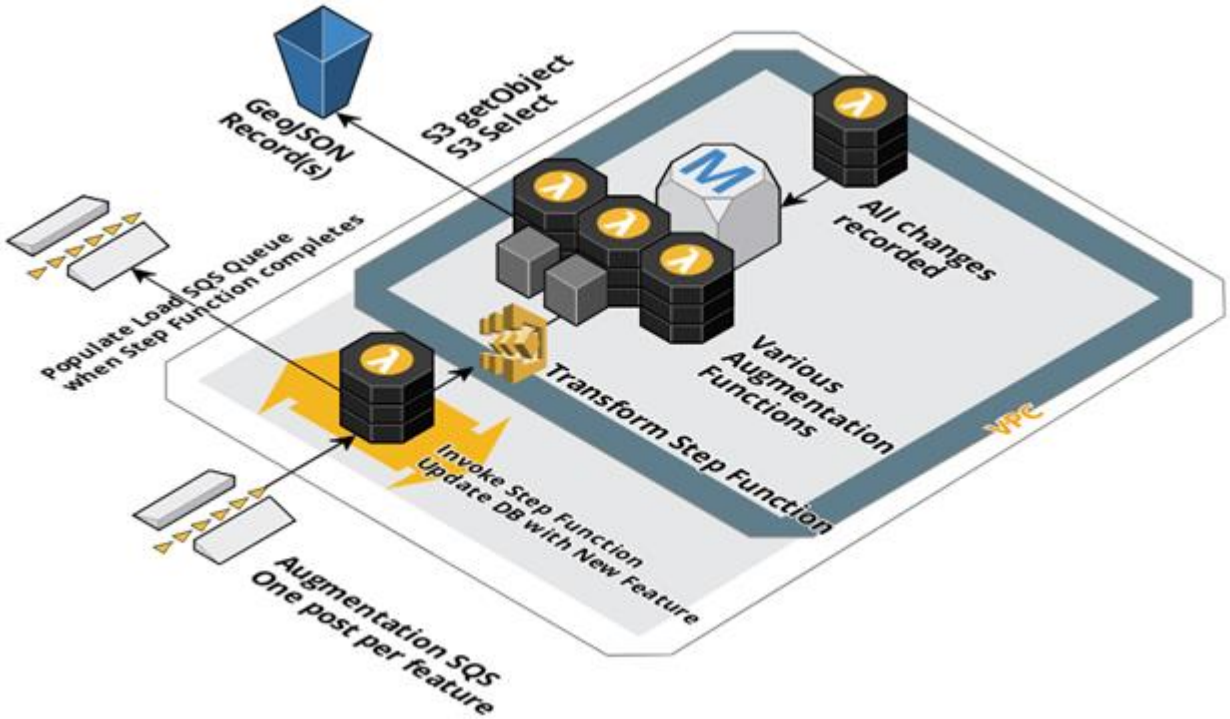


Figure 6 Location and Data Validation with Discrepancy Reporting inputs

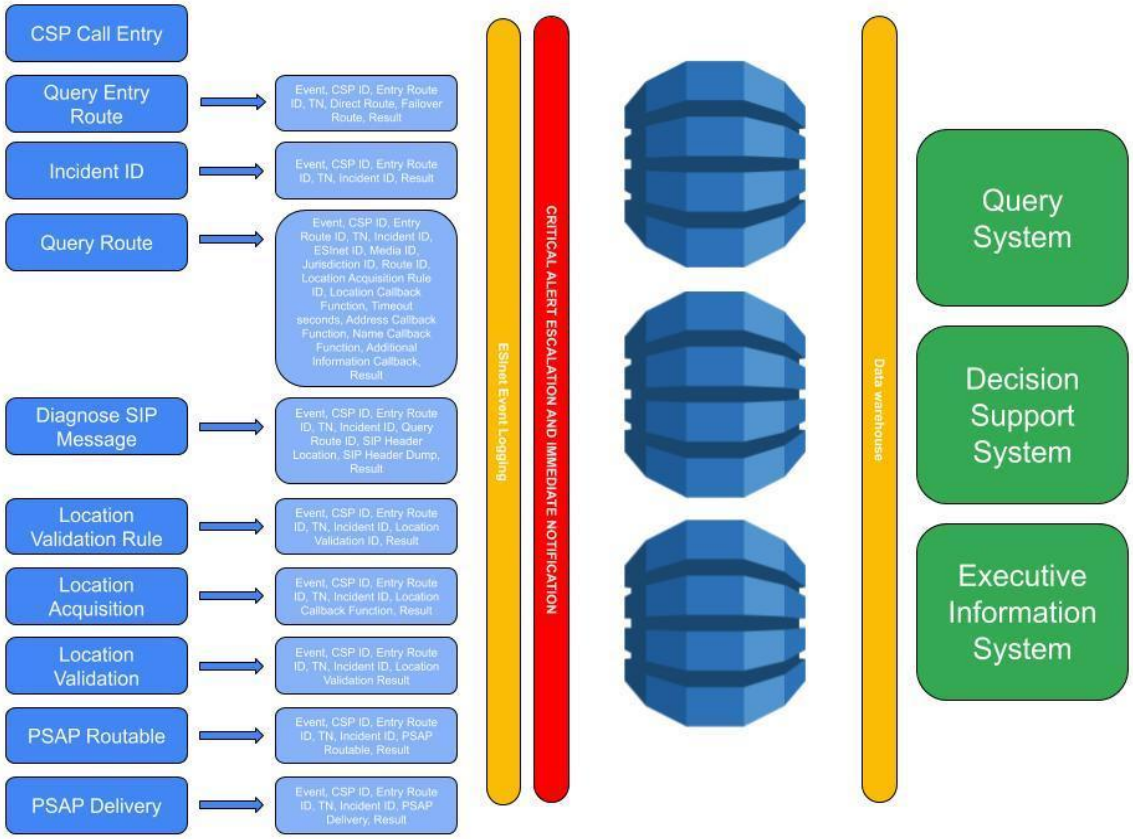


Figure 7 Alarm System Integration with Information Fusion and from Alarm, Security, and Telematics Companies

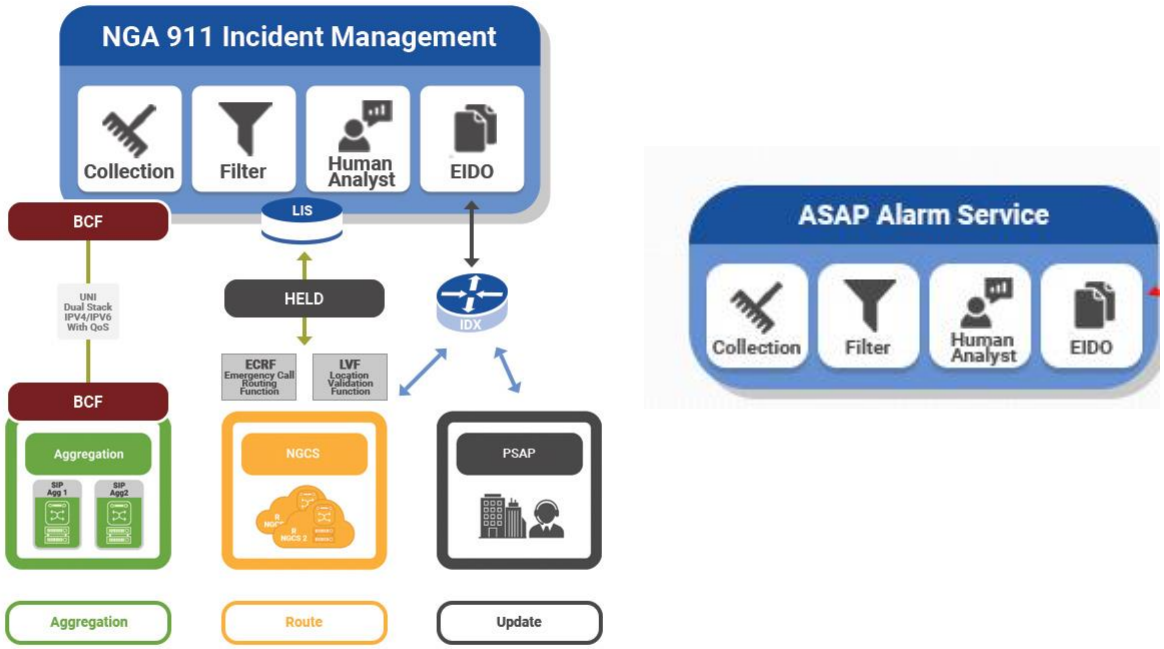
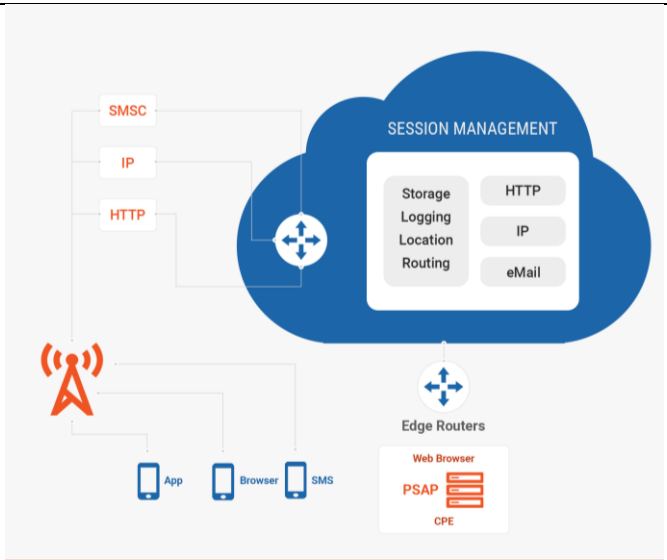


Figure 8 MSRP – for NGA 911 Text Control Center (TCC)



Legend:

a. Originating Service Provider (OSP) Connectivity -Figure 1;
The OSP traffic is depicted on the left side of the diagram and takes into account legacy, native SIP, and i3 formats

b. Legacy Network Gateway (LNG) – Figure 2;
The LNG is singled out in Figure 2 with an example of a wireless E911 ingress flow. (all configurations for wireline and VoIP are supported as well)

c. Border Control Function (BCF) – Figure 3;

d. Emergency Services Routing Proxy (ESRP) – Figure 1 and 4;

e. Policy Routing Function (PRF) – Figure 1 and 4;

f. Emergency Call Routing Function (ECRF) – Figure 1 and 4;

g. Location Validation Function (LVF) – Figure 1 and 4;

h. Spatial Interface (SI) – Figure 5;

i. Location Database (LDB) – Figure 1 and 4;

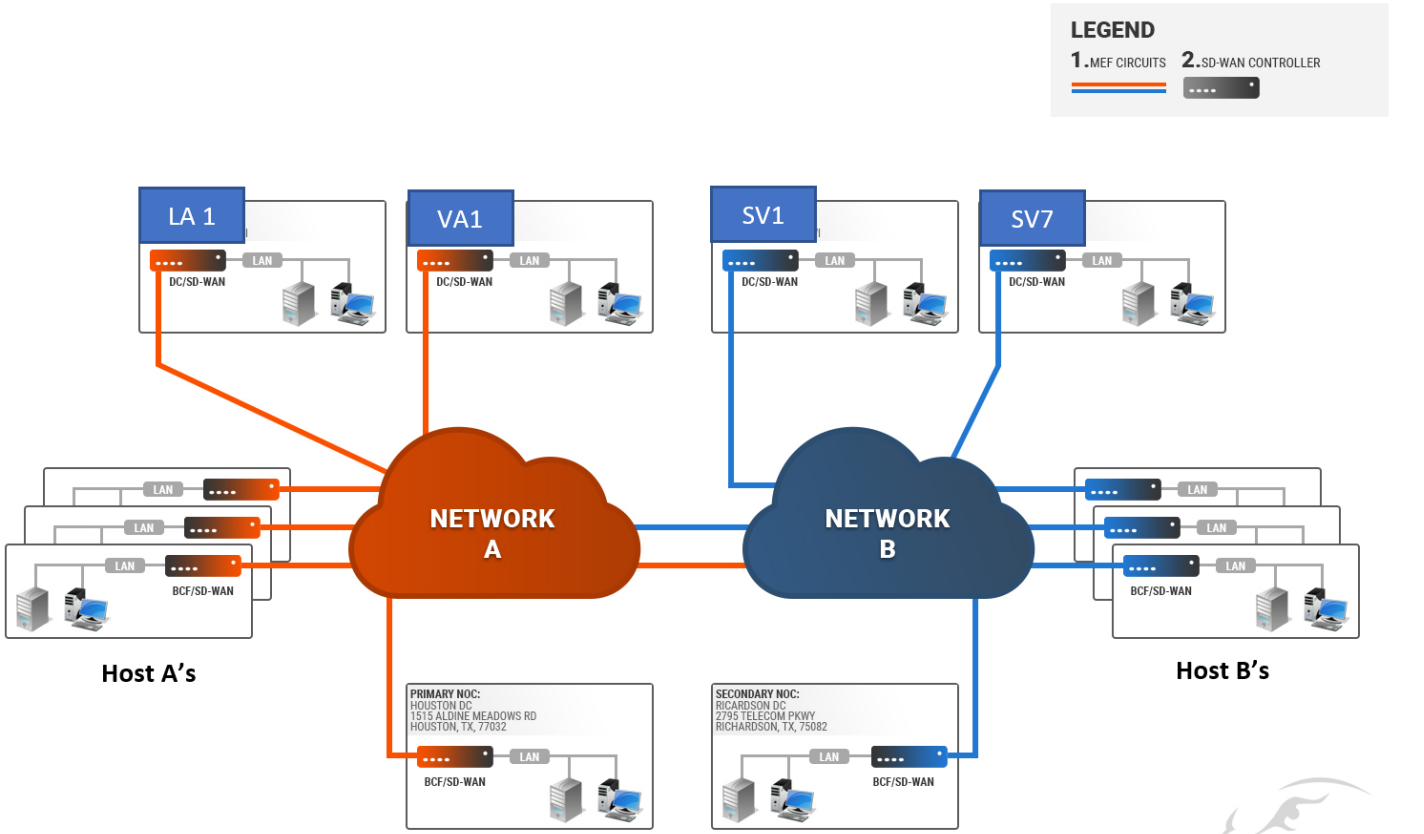
j. Discrepancy Reporting – Figure 1 and 6;

k. Logging and Recording – Figure 1 and 4;

l. Time Server – Figure 1;

m. Alarm Integration – Figure 7; and ,

	n Message Session Relay Protocol (MSRP) – Figure 8. Figure 9 The ESInet Connectivity for the NGSC Data Centers, redundant links, NOC/SOC to the Regional Serving Host Sites



Originating Service Provider (OSP) Connectivity Due Authorization

	NGA 911 will provide a copy of our current certificate of public necessity prior to award of contract. **Identification of Service Providers Connected to the Legacy Selective Router** NGA 911 takes full responsibility for identifying and for connecting all wireline, wireless, Voice over IP (VoIP), telematics, and other third-party service providers currently connected to the existing legacy selective router. NGA 911 will update this information quarterly for the term of the contract. We will provide a complete and updated service provider list for all connectivity to OSPs, POIs, SIP Aggregation, and to the PSAP Host Sites. Current providers include: • AT&T • CenturyLink • Verizon • Comcast • Charter • Inteliquent • Intrado • Commtech • Nitel • Frontier • Windstream • Etc.

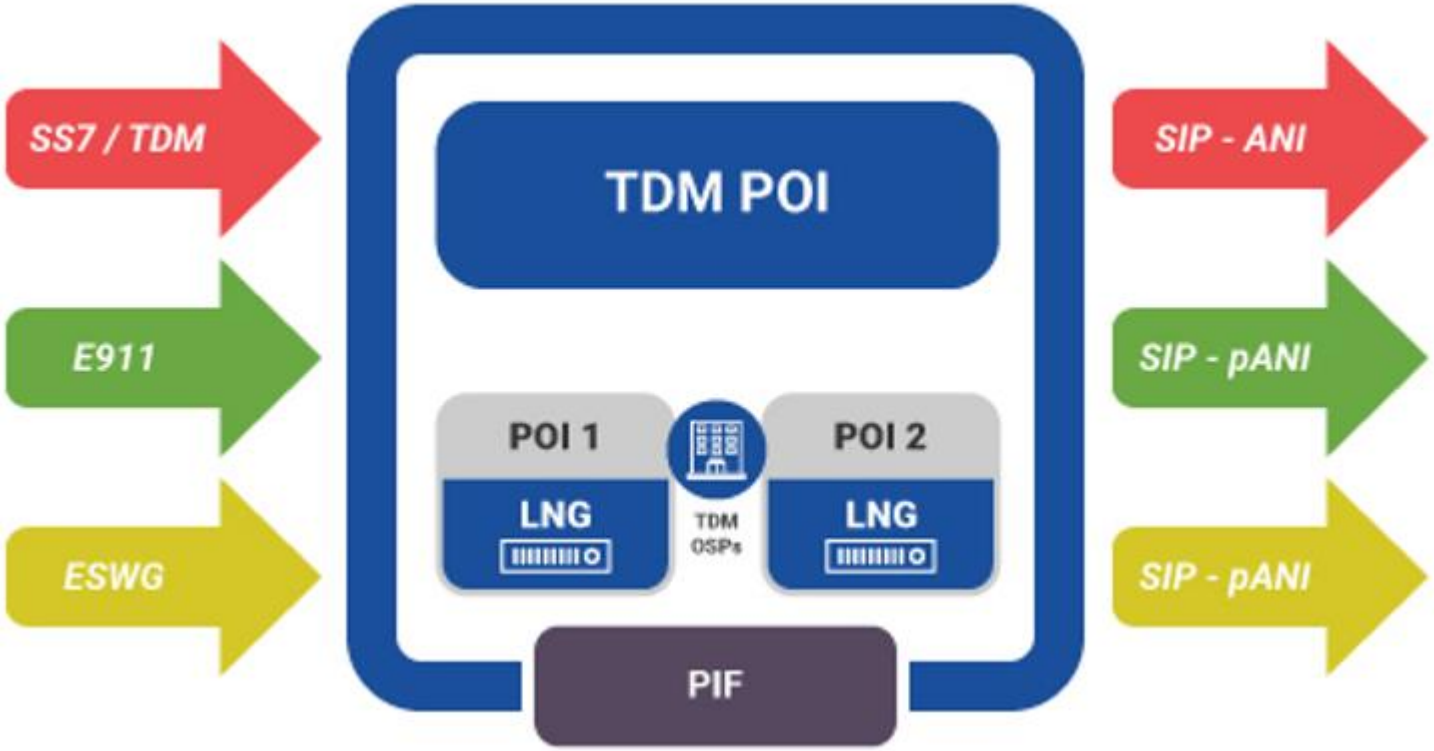
Any additional documentation can be inserted here

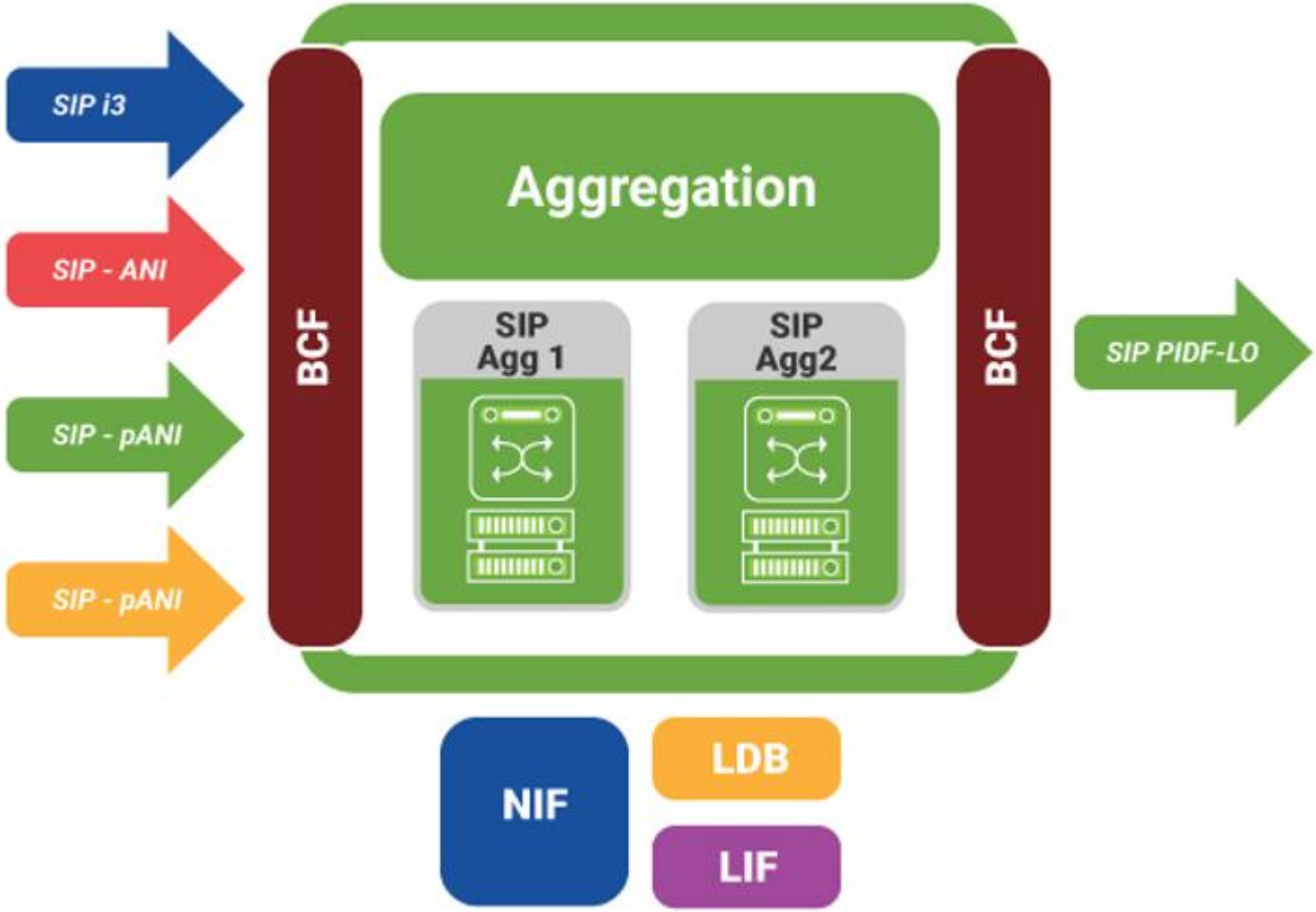
		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 2	**Next Generation Core Services Elements (NGCS)** **Interconnection and Commercial Agreements, and Trunking** **Originating Service Provider (OSP) Connectivity** Contractor shall be responsible for negotiating interconnection or commercial agreements, and for data and network connection arrangements with each service provider identified in requirement NGCS 1. Interconnection or commercial agreements shall cover subjects including, but not limited to, split rate centers and cell sectors, tandem-to-tandem connections to legacy selective routers and NGCS, Local Number Portability (LNP), National Number Portability (NNP), and Function of Code R (FoCR). Describe the process and provide timelines for meeting the requirements of this section, as well as the expected process for resolution of disputes.	X			
	Bidder Response: NGA 911 will be responsible for negotiating interconnection or commercial agreements, and for data and network connection arrangements, with each service provider in the State of Nebraska. The Interconnection or commercial agreements will cover subjects including, but not limited to, split rate centers and cell sectors, tandem-to-tandem connections to LSRs and IPSRs, local number portability (LNP), national number portability (NNP), and Function of Code R (FoCR). Below is a description of the process and estimated timelines for meeting the requirements of this section, as well as the expected process for resolution of disputes in the unlikely event that such would occur. Immediately upon contract award, NGA 911 will request interconnection agreements from the following service providers: • CenturyLink • AT&T • Consolidated Communications • Other ILECs It is anticipated attainment of interconnection agreements with the companies listed should take no more than four to six weeks to negotiate and execute, as these companies already have template agreements available. In any event, LECs and ILECs are compelled by the FCC to negotiate in good faith and are to provide timely interconnection negotiations to certificated carriers in accordance with "47 U.S. Code § 251/252". NGA 911 acknowledges the need for *split rate centers and cell sectors, tandem-to-tandem connections to legacy selective routers and IPSRs, local number portability (LNP), national number portability (NNP), and Function of Code R (FoCR)* to be a part of any agreement reached, and will strive to address each of these requirements in any agreements reached.				

	Although highly unlikely, should a *dispute* arise and the parties be unable to reach a timely agreement, NGA 911 will request the State Public Service Commission to arbitrate any remaining open issues after the 135th day after NGA 911's request for an interconnection agreement is received by the ILEC.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 3	**Next Generation Core Services Elements (NGCS)** **Originating Service Provider (OSP) Connectivity** **Management of OSP Connectivity** Contractor shall be responsible for managing moves, adds, changes, and deletions of the connections from the OSPs to the Contractor's systems for the term of the contract. Contractor shall allow for both Time-Division Multiplexing (TDM) and IP ingress to the network, proactively monitor these connections, and work with the respective service providers to resolve problems as they arise. Describe the process and provide timelines for meeting these requirements.	X			
	Bidder Response: NGA 911 will manage moves, adds, changes, and deletions of the connections from the Originating Service Providers to our Ingress and Aggregation POIs for the term of the contract. NGA 911 supports both TDM and IP ingress to the network, and proactively monitors these connections and works with the service providers to resolve problems as they may occur by providing network resources to troubleshoot and test connectivity. NGA 911 will work with the OSPs to receive network status. • The NGA 911 NG9-1-1 TDM Ingress POIs and the SIP Ingress POIs are designed to be highly available to operate on a 24x7x365 basis. • Below is a diagram of the typical TDM POI which together with our SS7 SCP provides for the PIF or protocol conversion to native SIP and SIGTRAN. • The SIP signals and associated ANI, pANI are forwarded to the SIP Aggregation Point for conversion into the i3 format through the LIF and NIF interworking. Native i3 will be passed through directly to the ESRP.				


SS7 / TDM
E911
ESWG
TDM POI
POI 1
LNG
TDM
OSPs
POI 2
LNG
PIF
SIP - ANI
SIP - pANI
SIP - pANI



Any additional documentation can be inserted here

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

NGCS 4	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **LNG Description** The LNG is a signaling and media interconnection point between callers in legacy call-originating networks, i.e., Enhanced 911 (E911), and the NENA NG911 i3 architecture. The LNG shall log all calls it receives and processes and shall permit the uploading of daily log files to a network monitoring and management system for analysis. The LNG shall allow for ad hoc uploads of log files for troubleshooting and incident response. All call activity on both the legacy side (TDM) and the IP side of the LNG shall be logged. The LNG shall have Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) functionality to detect and mitigate Distributed Denial of Services (DDoS) attacks from both the TDM side and the IP side. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			

Bidder Response:

The NGA 911 LNG(s) log all calls they receive and process and permit the uploading of daily log files to a network monitoring and management system for analysis. The LNG allows for ad hoc uploads of log files for troubleshooting and incident response. All call activity on both the legacy side (TDM) and the IP side of the LNG shall be logged. The LNG is integrated into our NOC and SOC with intrusion detection system (IDS)/intrusion prevention system (IPS) functionality to detect and mitigate distributed denial of service (DDoS) and telephony denial of service (TDoS) attacks from both the TDM side and the IP side.

NGA 911 will deploy the POI by working with each of the OSPs and particularly the major ILECs. NGA 911 has already developed and implemented a formal approach to engaging the OSPs for California, West Virginia, Louisiana, and Nevada. NGA 911 will replicate this process for Nebraska. The NGA 911 approach is to encourage a transition to i3, but we are prepared under the guidance of the Commission, to deploy POI's in the LATAs (for ILECs) and configure the LNGs through a rigorous Product Realization process to reliably provide PIF for delivery of a SIP call (over an NG Trunk if necessary) to the SIP Aggregation Service where NIF and LIF will be carried out as required to generate as best as possible an i3 SIP INVITE (in a format defined. specified, tested and accepted by the Commission). Phase 1 and 2 E911 wireless OSPs will be asked to deliver their calls to the POIs located at the Aggregation Services Data Center but will have the option of meeting at any qualified POI in the State.

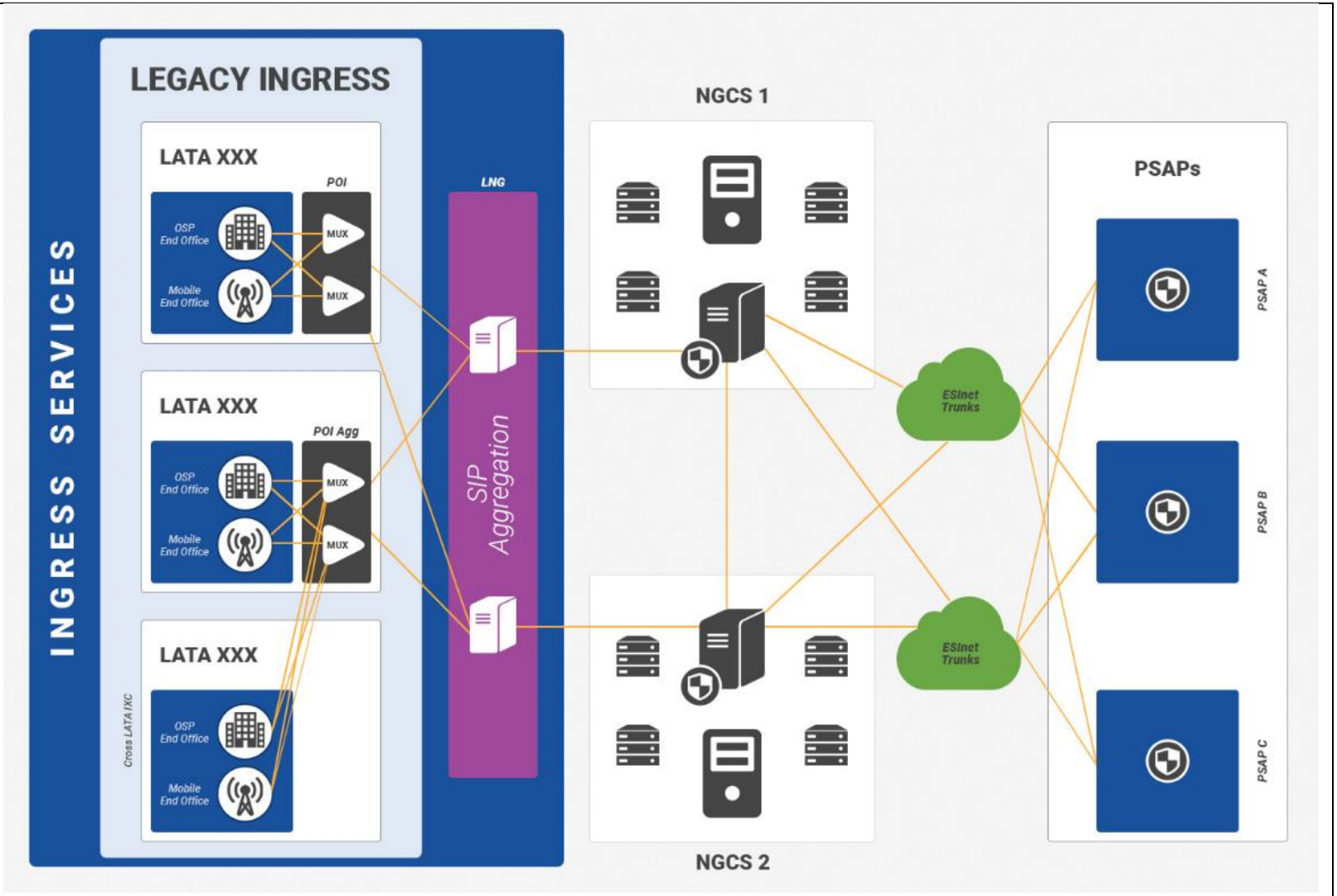
Monitoring, Detecting and Mitigating DDOS, TDOS and other Attacks

The NGA 911 Security Operations Center (SOC) monitors the authorized use of the network including DDOS, TDOS, and other attacks. Should identification of a vulnerability or a threat occur, we perform the initial and emergency response to the security event and in less than 24 hours provide the Commission a document describing the measures taken, and any additional implementation plans to avoid a breach entirely.

Upon detection, the SOC and operations are secured by Network Segregation techniques in an active-active network where media is sent across to distinct paths. A disruption of one is not necessarily impacting the other. The IPS, AI, and network monitoring isolate the source

	of the DDOS and TDOS threat and segment the traffic immediately. In almost all cases the source of such attacks is through the ingress network and the source OSP will be identified and notified. The FE's in the affected core are isolated and if possible, traffic from that OSP is handled. If necessary, the offending OSP's traffic will be blocked until working together with the OSP, the NOC, SOC, and the Commission the threat is eliminated and the OSP is allowed back on the network.

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 5	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** Contractor shall provide redundant, resilient LNGs with legacy selective router gateway (LSRG) functionality to allow the legacy selective routers to transfer calls with Automatic Number Identification (ANI) and Automatic Location Identification (ALI) information to deployed NGCS and vice versa. Legacy functionality and components shall be in place and operational during the NG911 transitional phase until all 911 authorities and PSAPs served by the legacy selective router have completed the transition. Describe the steps bidder will take to meet the transition timelines and minimize overlapping network costs.	X			
	Bidder Response: NGA 911 provides redundant, resilient LNGs with LSRG functionality to enable the LSRs to transfer calls with automatic number identification (ANI) and automatic location identification (ALI) information to deployed NGCS and vice versa. Legacy functionality and components shall be in place and operational during the NG9-1-1 transitional phase until all 9-1-1 authorities and PSAPs served by the LSRs have completed the transition. The LNG/LSRG are currently supported on a national meshed network.				


INGRESS SERVICES
LEGACY INGRESS
LATA XXX
POI
OSP End Office
Mobile End Office
MUX
MUX
LATA XXX
POI Agg
OSP End Office
Mobile End Office
MUX
MUX
LATA XXX
OSP End Office
Mobile End Office
Cross LATA IXC
LNG
SIP Aggregation
NGCS 1
NGCS 2
ESInet Trunks
ESInet Trunks
PSAPs
PSAP A
PSAP B
PSAP C

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

Any additional documentation can be inserted here

	Next Generation Core Services Elements (NGCS) **Legacy Network Gateway (LNG)** **Previous Work on Similar Solutions** 1. Explain how bidder has worked with legacy OSPs with similar solutions on similar projects. 2. Submit specific plans for working with established legacy 911 service providers in Nebraska.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 6		X			

Bidder Response:

NGA 911 is unable to provide specific plans from our work with established legacy 9-1-1 service providers in Nebraska because NGA 911 is under NDA with those providers and this would be a violation of the NDA. However, upon contract award NGA 911 will be able to leverage those plans and experience in Nebraska.

There are several steps and milestones necessary to complete an OSP migration from the existing legacy network to the NGA 911 ESInet/NGCS. Given our current knowledge, in the best case, it will take 6-9 months to interconnect the OSPs including testing and validating the trunks. Should any OSP facilities have build out delays, it could take up to a year. There is a lot that will not be known until the actual orders are entered, and the OSP returns a firm order commitment date.

But our work in CA, NV, WV, and FL means that we are regularly meeting with a large number of OSPs and for each of these we have plans, and for those that are also in Nebraska we will be able to leverage those plans.

We have also provided additional information for your review.

Best Case Scenario

It would be feasible to start asking OSP's to interconnect to two (2) NGA 911 provided POIs within 4-6 months of contract award. There are 26 OSPs operating in the Nebraska region. Many of these end office switches are not digital switches and are reliant on the 5ESS digital switch to provide an SS7 interconnection to the NGCS POI. NGA 911 will work with AT&T to provide an aggregation service from the existing 5ESS where these carrier end offices converge. This method will speed the conversion as well as provide a more systematic route conversion point. If the 5ESS can be used for an aggregation point, NGA 911 estimates that conversions could start happening in the 6-9-month period.

Wireless OSPs will be encouraged to interconnect with IP/SIP, which may speed along the interconnection efforts. Note that migration is not a serial process. There will be instances that OSP traffic supporting a particular PSAP has been migrated, thus allowing that PSAP to be migrated earlier. There will be provisions made between the NGCS and the Legacy Selective Router to transfer calls between PSAPS during the migration period.

Worst Case Scenario

Should we not be able to use the 5ESS switch for aggregation, each individual END office would need to provision new trunks to the NGA 911 POI. Preliminary numbers look like that would be approximately 86 OSP interconnections. Depending on the rate at which OSP's can build out these connections, this would delay the conversion process to an estimated 12 months. Note that this is an estimate, and we are unable to pre-determine what issues may occur with an OSP until the actual circuit order is put in, and we are given a firm order commitment (FOC) date from the OSP.

Integration of all OSP connectivity for wireline, wireless, and VoIP traffic, as well as multiline telephone systems (MLTS)
NGA 911's approach takes into consideration that not all OSPs will be capable of SIP delivery. Although some will, including many MLTS solutions. Construction of SS7 and SIP Aggregation Points, along with the conversion of SS7 to SIP, for Nebraska are critical milestones of the IP cutover strategy where the Selective Router is left as a split wire center with a supporting LSRG.

Legacy and SIP Aggregation Services are Mutually Exclusive Services: NGA 911 provides both Legacy and i3 aggregation services for all Wireline, Wireless, VoIP, and MLTS served by Nebraska. For Legacy, NGA 911 will identify POIs for legacy traffic to convert to i3 through a fully functional LNG (PIF at POI, NIF, and LIF at Aggregation Point) supported by an LDB.

Redundant (at least two) TDM POIs established in the region to process SS7 calls using an LNG and deliver them to the redundant SIP Aggregation Points.

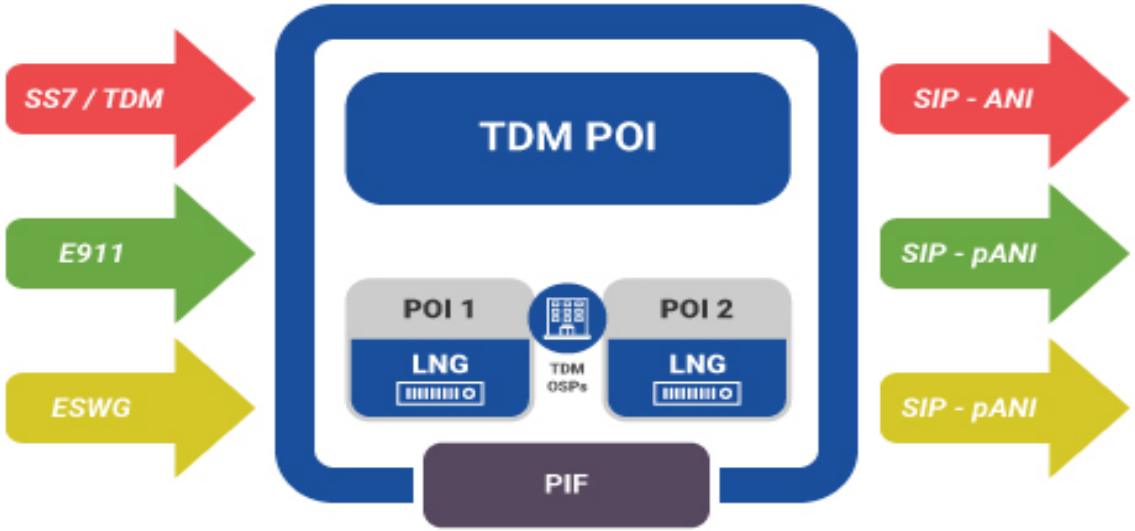
Letter of Authority

NGA 911 will coordinate with Nebraska to obtain a Letter of Authority to allow us to communicate directly with the OSPs on behalf of Nebraska.

Establish Interconnection and Commercial Agreements, and Trunking
NGA 911 currently has interconnect agreements and trunking arrangements with multiple service providers including Verizon, AT&T, CenturyLink, and Frontier. NGA 911 will negotiate any additional interconnect agreements and trunking arrangements as needed.

Immediately upon obtaining a Certificate of Convenience and Necessity (CCN) from the Nebraska Public Service Commission, (in process) NGA 911 will request interconnection agreements specific to Nebraska from the following service providers:

	• CenturyLink • Windstream • Alltel • Verizon • AT&T • T-Mobile • Sprint • Any other identified Anticipated attainment of interconnection agreements with the companies listed should take no more than six weeks to negotiate and execute, as these companies already have template agreements available. NGA 911 acknowledges the need for split rate centers and cell sectors, tandem-to-tandem connections to legacy selective routers and IPSRs, local number portability (LNP), national number portability (NNP), and Function of Code R (FoCR) to be a part of any agreement reached, and will strive to address each of these requirements in any agreements reached. Although highly unlikely, should a dispute arise and the parties be unable to reach a timely agreement, NGA 911 will request the Nebraska Public Service Commission to arbitrate any remaining open issues on the 135th day after NGA 911's request for an interconnection agreement is received by the ILEC. Coordinate with all telecommunications providers and manage circuit order processes to include testing and integration NGA 911 will coordinate with all telecommunications providers and manage circuit order processes to include testing and integration. NGA 911 will assign a NG Trunk Coordinator. The NG Trunk Coordinator will be responsible for, but not limited to: • Manage FOC dates with carriers • Coordinating site walk throughs (if requested by provider) • Coordinating Installation and Testing • Coordinating Integration and System Testing • Communication with the NGA 911 Project Manager to provide status of circuit order and installation The NGA 911 NG9-1-1 TDM Ingress POIs and the SIP Ingress POIs are designed to be highly available to operate on a 24x7x365 basis. Below is a diagram of the typical TDM POI, which, together with our SS7 SCP POIs provides for the PIF (protocol conversion) to native SIP and SIGTRAN.



Any additional documentation can be inserted here

	Next Generation Core Services Elements (NGCS) **Legacy Network Gateway (LNG)** **Traffic Engineering Process** Describe the process that will be utilized to analyze the current trunk engineering for 911 traffic, and to validate any applicable trunk rebalancing for public-safety grade service.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 7		X			

Bidder Response:

NGA 911 relies on the Erlang C formula when making traffic dimensioning decisions. Erlang C is a proven reliable way to make a determination on the number of trunks needed to support a given load and balanced by the number of available positions. With an initial provisioning of 10 Mbps at each PSAP, trunking should not be a problem in any case, where 10 Mbps can support between 500 to 5000 simultaneous calls depending on codec.

The Erlang C formula expresses the probability that an arriving customer will need to queue (as opposed to immediately being served). Just as the Erlang B formula, Erlang C assumes an infinite population of sources, which jointly offer traffic of A erlangs to N servers. However, if all the servers are busy when a request arrives from a source, the request is queued. An unlimited number of requests may be held in the queue in this way simultaneously. This formula calculates the probability of queuing offered traffic, assuming that blocked calls stay in the system until they can be handled. This formula is used to determine the number of agents or customer service representatives needed to staff a PSAP, for a specified desired probability of queuing.

$$P_W = \frac{\frac{A^N}{N!}\frac{N}{N-A}}{\left(\sum_{i=0}^{N-1}\frac{A^i}{i!}\right) + \frac{A^N}{N!}\frac{N}{N-A}}$$

where:
- A is the total traffic offered in units of erlangs
- N is the number of servers
- PW is the probability that a customer has to wait for service.

In order to maintain a Public Safety Grade of Service (GoS) the following will be determined: the length of time call takers and dispatchers spend on a call, the number of erlangs (A) that remain on the EO and CAMA trunks, the Public Safety Grade acceptable response time (Pw) and the number of available call takers (N).

NGA 911 follows this formula to analyze the current trunk engineering for 9-1-1 traffic, and to validate any applicable trunk rebalancing for public safety-grade service. The NGA 911 solution is scalable and can seamlessly accommodate additional bandwidth as needed.

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 8	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Location Information** The LNG shall obtain location information to define, create, populate and send the correct Presence Information Data Format Location Object (PIDF-LO) parameter to the correct ESRP or terminating PSAP, as described within NENA-STA-010.2-2016. Describe how the solution meets or exceeds the above requirements.	X			

Bidder Response:

The NGA 911 LNG provides a fully functional LIF (location interworking function) supported by a comprehensive transitional Location Database (LDB).

The LDB is available to Originating Service Providers (OSPs) so they can verify that civic addresses will return PSAP or emergency responder URIs either using an Application Program Interface (API) Gateway or through an NGA 911 provided web-based solution from our partner COMsolve. The choice of which method used is determined by the needs and requirements of the OSP.

LDB/LIS: Exceeding requirements, the LDB/LIS we are providing serves civic addresses and includes support for E911 and i2 as well. These additional features enhance ingress routing for all legacy providers, wireline, wireless and VoIP. The enhanced LDB/LIS covers every scenario for supporting the LNG in the formulation, attachment, and delivery of a valid PIDF-LO compliant Header to the ingress ESRP. For this reason, our LDB/LIS maintenance and support interface provides for not only the verification of civic addresses, but also ESRK, ESRD (pANI) for E911, and ESQK for i2.

LDB Initial Load(s): In preparing the LDB as the routing database for legacy OSPs, locations and keys will initially be ingested in bulk and verified against a data dump from the existing legacy ALI/MSAG/SRDB. Given the diverse sources of this information these loads will not necessarily all be completed at one time. Different parties will be required to verify the data sets relevant for their client records including OSPs, MPC/GMLC's VPC, and other location key and data providers. Verification will depend on the type of service provided whether it is an actual civic address, or a key range. Civic addresses and key ranges are associated with PSAP routing boundaries in the GIS and updated in the LVF validation data prior to being active in the LDB. The process is complete when an input from an OSP or Location Service Provider regularly and uniquely returns the correct emergency responder URI associated with a PSAP endpoint.

Regular LDB Maintenance (Diagram 21.0.8.1): After initial loading, verification and validation, the LDB must be regularly updated by the OSPs and Location Service Providers. NGA 911 offers a number of different options for the LECs to manage their Service Order Input (SOI) Updates. Proper updating requires adherence to a process to ensure data is ingested and the LDB integrity is protected. The OSP sends data to NGA 911 by one of the available ingest methods. The SOI files are loaded into the NGA 911 COMsolve system for processing. The SOI updates validate against the different databases and tables depending on the source and LDB category of the input, if a record passes all validations, the update is applied to the LDB. If the record does not successfully pass all

	required validations, an error is returned with error codes associated with the specific error type and the update is not applied to the LDB until the error is resolved. **Intuitive Interface (for Web Upload Product – Diagram 21.0.8.2):** The COMsolve Web input system automates either single site or batch of the following operations and activities: • **Civic Address management (SOI)** features include add civic address, validate address is resolvable in GIS, update the LVF and activate in the LDB; • **ESRK/ESRD management** features include add ESRK/ESRD range, for ESRD implementations, allocate ESRDs to cell tower, for ESRK implementations - link ESRK range to PSAP and allocate cell tower to appropriate ESRK range, monitor ESRKs/ESRDs level, and warn when ESRK/ESRD levels are low; • **9-1-1 routing table** import updates to routing tables, determine required changes, reassign ESRK Ranges/ESRDs, determine if new 911 trunks are needed, generate LDB list load files to include local address verification function (LVF) pre-check against GIS database where results are made available to OSP, and can be used to update LDB for fixed line applications (ports, adds, disconnects). **CPE that do not support PIDF-LO:** The properly configured LDB and the resulting PIDF-LO from the LIF can also be used to support an LPG at PSAPs that still use legacy equipment and may require an ALI, E2, or V2 dip for address updating, A similar function will be provided for non i3 SIP based CPE that also require access to an ALI formatted feed.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 10	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Protocol Conversion** **External Interfaces** The LNG external interfaces shall comply with NENA-STA-010.2-2016, requirements SLA 1-23, and other applicable standards and requirements. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The NGA 911 LNG fully complies with NENA-STA-010.2-2016, and considers the criteria identified in NENA-INF-008.1 and CSRIC 6 Final Report – Recommendations for 9-1-1 System Reliability 4 and Resiliency during the NG9-1-1 Transition. NGA 911 is committed to meeting or exceeding SLAs defined in 1 through 23 and specifically here, those that relate to the LNG and other transitional functions and elements. NGA 911 understands that the LNG external shall comply with respective NENA requirements and will comply. The LNG offered in this proposal offers external interfaces for SS7 and CAMA. For OSPs interconnecting via TDM, most if not all will choose to interface via SS7.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 11	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Baudot Code Transcoding** The bidder's BCF solution shall support transcoding of Baudot tones to real-time text (RTT), as described in IETF RFC 4103. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: NGA 911's BCF is capable of translating Baudot tones received from a TTY or other carrier system into real-time text (RTT). NGA 911's solution supports transcoding of non-IP text to IP-based real-time text, as described in IETF RFC8 4103 and IETF RFC 5194, and can support other applicable standards associated with real-time text. The NGA 911 solution and Border Control Function (BCF) are fully compliant with National Emergency Number Association (NENA) Detailed Functional and Interface Standards for the NENA i3 Solution NENA-STA-010.2-2016. The BCF provides the functionality to maintain logs of non-IP text transcoding of all 9-1-1 sessions and all additional BCF logging and recording requirements, which are maintained by the NGA 911 Network Management Information System (NMIS).				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 12	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Callback Number** The LNG shall support obtaining the callback number associated with any pseudo ANI data that does not include the callback number. This may require the Contractor to obtain the callback number from the wireless or VoIP provider and may include additional recurring and non-recurring costs that are independent of this RFP. The Contractor shall be responsible for all recurring and non-recurring costs associated with this requirement. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: NGA 911 will provide a fully functional LNG to include the LIF and ADRs that are derived from the TN or a pANI. The Call Back Number will be retrieved from the MPC, GMLC, VPC, or in some transitional cases by other means as detailed in our agreements with the MSO (mobile service operators) and location positioning centers. Call back numbers in the NGCS are updated in an ADR by reference and/or the PAI. The LNG is capable of querying a wireless carrier's MPC or GMLC and a VoIP Service provider VPC to obtain a callback number. These functions are all included in our proposal and NGA 911 will not pass on any additional recurring costs associated with this function.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 13	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Event Logging** The LNG shall facilitate logging of all significant events and 911 calls received and processed. Each call log shall contain all relevant parameters defined in Section 5.13.3 of NENA-STA-010.2-2016. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The NGA 911 LNG facilitates the logging of parameters including those defined in Section 5.13.3; however, in legacy systems not all of the fields defined in NENA-STA-010.2-2016 are available from a TDM based OSP without the addition of data from the LDB, an MPC, VPC, and other data sources. NGA 911's solution collects and prepares an i3 SIP INVITE with all possible fields at call delivery to the NGCS. Nonetheless additional data may be gathered later and logged in the MIS and CDRs for each call. In some cases not all fields are available due to OSP limitations – these will be noted in the log and by class of service when necessary.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 14	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Extraction of Log Files** All LNG log files shall be capable of being extracted in near real-time and shall be in a format suitable for importing into a spreadsheet or word-processing program. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: NGA 911's LNG log files can be extracted in near real-time and delivered either through the portal or download in an .xls, .pdf, or a .csv format suitable for importing into a spreadsheet or word-processing program.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 15	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **High-Availability Design** The LNG solution shall be deployed in a high-availability design to meet public safety-grade resiliency and redundancy requirements, Section V.D.1.b. (General Requirements – Technical – Public Safety Grade). Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: NGA 911 designs, engineers and deploys our LNGs diversely in a minimum of two data centers to exceed Public Safety Grade as defined in Section V.D.1.b. of the RFP. NGA 911 exceeds five 9's reliability and availability. The data centers never rely on a single network service provider for connectivity where we aggregate and bond broadband trunk circuits from at least 3 providers. On the network side, our infrastructure is geographically diverse and built in two regions and four availability zones. The LNGs are dimensioned to cover more than 200% of the call volume of the attached OSPs and can be scaled up easily in the face of an unanticipated spike in demand.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 16	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Legacy Selective Router Gateway (LSRG) Functionality** The LSRG functionality shall support selective transfer, commonly referred to as "star code" transfers, made by legacy PSAPs for calls destined for the NextGen911 PSAPs or to neighboring legacy PSAPs outside of the ESInet. Describe how bidder's LNG solution provides for LSRG functionality.	X			
	Bidder Response: The LSRG offered in this proposal supports star code transfers for a participating NG PSAP to a non-participating Legacy PSAP or from a non-participating Legacy PSAP to a participating NG PSAP. Conversion from SIP to TDM or TDM to SIP maintains the information required for the transfer. This feature is priced to cover transfers to and from the legacy selective router providing service to the State of Nebraska. This capability can be extended to transfers to legacy PSAPs served by other legacy selective routers. The LNG and LSRG share many common features. However, the LNG is uni-directional. Calls come in, get processed, and exit on their way to the ESRP. LSRGs are bi-directional. Calls can be presented to the LSRG from either the TDM side or the SIP side. The carrier-grade Sonus GSXs can be deployed in either configuration.				

Any additional documentation can be inserted here

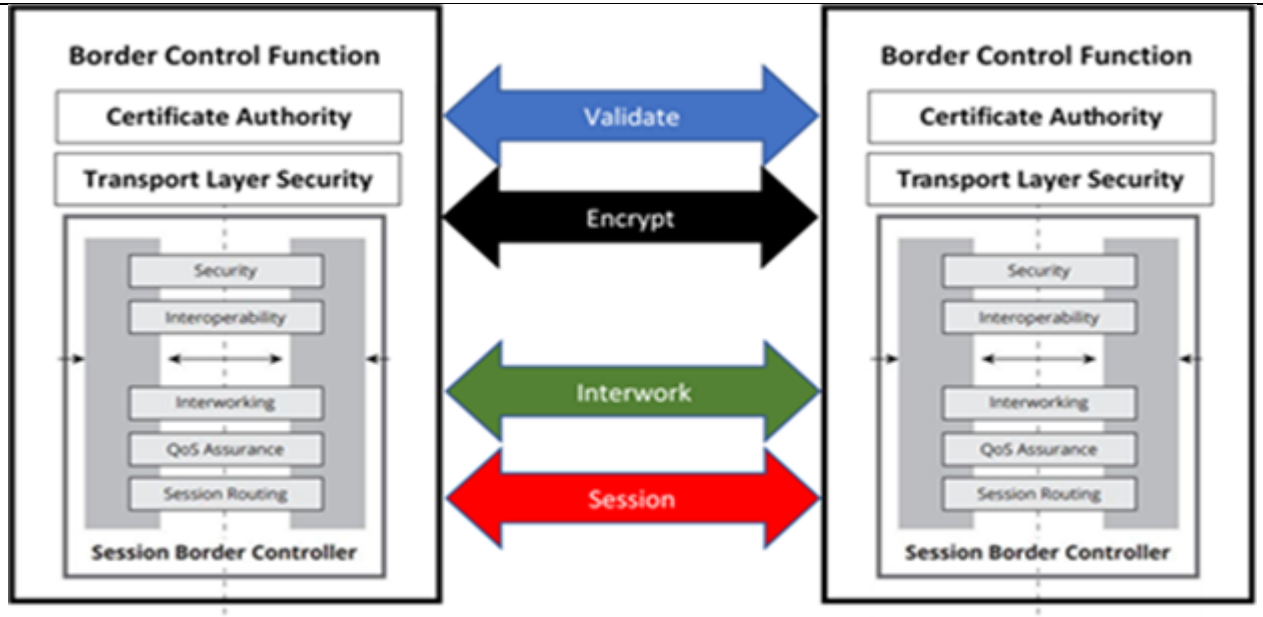
		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 17	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Proposed LNG Locations** Provide the proposed locations for hosting the primary LNGs for the NextGen911 system, including the data center tier level for the host sites.	X			
	Bidder Response: The LNG's will be hosted in at least two-Tier 3+ data centers that are geographically diverse including options for Denver, Dallas, Los Angeles, Phoenix, Minneapolis and Chicago among others. The Data Centers are on a national TDM network providing for in state POIs on Net with CenturyLink, Windstream and the wireless carriers as necessary. Smaller CLECs and ILECs may opt for an aggregator like Bandwidth or Inteliquent to deliver traffic to NGA 911 as we have seen in other states.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 18	**Next Generation Core Services Elements (NGCS)** **Legacy Network Gateway (LNG)** **Charges for Dual Service** The bidder shall be responsible for meeting the timelines outlined above in requirement NGCS 2 and 3. If the transition from the legacy selective routers to NGCS exceeds the committed timeline, and is attributable to the acts or omissions of the Contractor, the Contractor will accept responsibility for financial support of the legacy network until such time as the full transition is complete. Describe how bidder's solution meets this requirement.	X			
	Bidder Response: NGA 911 will be responsible for meeting the timelines outlined above in requirements NGCS 2 and 3. If the transition from the legacy selective routers to NGCS exceeds the committed timeline, and is attributable to the acts or omissions of NGA 911, NGA 911 will accept responsibility for financial support of the legacy network until such time as the full transition is complete.				

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 19	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **BCF Description** The BCF shall provide logical network security functions between external networks and the ESInet, and between the ESInet and PSAP networks. The BCF is responsible for numerous functions, including the following: a. Border firewall; b. VPN; c. IDS/IPS; d. Session Border Control (SBC); e. Opening and closing of pinholes; f. Limiting access to critical components through the use of VLANs; g. Call admission control; h. Media transcoding; i. Signaling protocol normalization and interworking; j. Network Address Translation (NAT); k. Codec negotiation; l. Support for QoS and priority markings; and, m. Media proxy. Provide details, including drawings, describing how the proposed BCF meets or exceeds all functions listed above and the requirements described in NENA-STA-010.2-2016, as well as additional firewall requirements described in NENA 04-503, NENA-INF-015.1-2016, and NENA 75-001, or the next subsequent version of the NENA documents listed that are publicly available at the proposal release date.	X			
	Bidder Response: The BCF provides logical network security functions between external networks and the Ingress Network, and between the Ingress Network and The State of Nebraska networks. The BCF is responsible for numerous functions, including the following: NGA 911 utilizes carrier class BCF's to provide a uniform network interface with comprehensive security features when linking between Next Generation Network Domains including VoIP, SIP, HTTPS interfaces and VoLTE / IMS networks. Network signaling and media settings are deployed through a comprehensive OA&M web-based interface. The BCF exceeds all functions listed above and the requirements described in NENA 08-003 (superseded by NENA STA-010.2-2016 and soon STA-010.3), as well as additional firewall requirements described in NENA 04-503 and NENA 75-001 (NG-SEC). The BCF is the interface of two disparate networks that negotiate, limit, regulate, and secure traffic based on authentication, authorization, traffic type, ports, address-translation, QoS, and session. In i3, the BCF provides border functionality between the				

	Ingress Aggregation Network, other ESInets, member PSAPs, permitted foreign functional elements such as ESRP's, LIS's, and authorized API's for the purposes of report querying. Ideally, all interactions with the BCF are secured by credentials issued by the PSAP Credentialing Agency (PCA); but as of yet the PCA has not been established; so, all BCF-to-BCF interfaces will be bilaterally negotiated and credentialed by mutual agreement in the meantime. The NGA 911 BCF functionality addresses the requirements at the boundary where different service provider or peer networks interconnect to the NGCS. The NGA 911 BCF provides security for your NGCS in terms of signaling information by implementing a Topology-Hiding Inter-network Gateway (THIG) sub-function. This sub-function performs signaling-based topology hiding, IPv4-IPv6 interworking and session screening based upon source and destination signaling addresses. It also utilizes an inter-working function when connecting non-SIP or non-IPv6 networks. It also interacts with the transport boundary at layers 3 and 4 for control of the boundary at the transport layers including pinhole firewall, Network Address and Port Translations (NAPT) and numerous other features. Quality of service (QoS) packet marking, bandwidth policing, usage metering and QoS measurements for the media flows are additional features supported by the BCF. The NGA 911 solution does not require physical equipment/hardware. The BCF is implemented as a Virtual Network Function (VNF) Appliance in the Amazon Web Service (AWS) Cloud. Entities outside the ESInet will be required to provide their own BCF/SBC which may be of any make and manufacture that complies with NENA and IETF interworking requirements.



The BCF through the Session Border Controller (SBC) function acts as a border firewall in support of direct connect and/or a VPN endpoint. The BCF provides monitoring and intrusion detection and protection (IDS/IPS). By acting as a DMZ access to critical components are protected by using VLANs which also limits access to critical components.

The SBC also provides call admission control, media transcoding, signaling protocol normalization and interworking, network address translation (NAT), codec negotiation, support for QoS and priority markings, and also as a media proxy and a back-to-back user agent.

In accordance with NENA i3, the BCF provides for authorized entry into the Ingress Network for emergency calls presented to the network as long as the originating network provides valid certification. The BCF incorporates firewall, admission control, and may include anchoring of session and media as well as other security mechanisms to prevent deliberate or malicious attacks on PSAPs or other entities connected to the Ingress Network. Until the PCA is established NGA 911 will work bilaterally with all potential call "presenters" to facilitate strictly secure and authenticated access to the State's Ingress Network for the purposes of 9-1-1 call delivery.

- SIP Trunks

	• Lawful Intercept - ETSI compliant LI solution
	• Security - up to the minute security features including firewall and DOS, DDOS
	• Interworking - fully compliant SIP, SIP-I, SIP-T, H.323, IPv4, IPv6
	• Topology Hiding
	• Scales from 500 to 30,000 simultaneous calls
	• Capable of handling 600 Calls Per Second
	• Support for up to 250,000 subscribers
	• Media - support for industry leading codecs and RTP encryption
	• Operating Modes - full support for Stateful / Stateless proxy mode and B2BUA
	• Comprehensive web-based operation
	• Redundant Architecture – Full redundancy support for automatic failover. Ensures five 9s (99.999%) reliability at network edge (see next section).
	• RTP Failover and Re-Invite
	• Capacity Growth – Distributed
	• Full Class 4 SoftSwitch capabilities
	  ○ Powerful Routing Capabilities
	  ○ Optional SS7 Interconnect
	• Security
	  ○ SBC DoS/DDoS protection
	  ○ Allow trusted/authenticated users access while under DoS attack
	  ○ Dynamically accept or reject traffic based on device behavior
	  ○ Throttling & Overload Protection
	• Topology Hiding and Privacy
	  ○ Hide network topology preventing direct attacks and maintain privacy
	  ○ Mask user information for privacy and confidentiality
	• Access Control
	  ○ Control of max concurrent sessions
	  ○ Filter devices/networks on a per application basis
	  ○ Permit access to known devices or networks
	  ○ Authorize/deny access for registered users; permit or deny access to mask users
	  ○ Dynamically accept or reject traffic based on device behavior
	  ○ Accept media only for authorized sessions
	• Fraud Prevention
	  ○ Perform signaling and media validation by authenticating and authorizing users

	VoIP Signaling Protocols • SIP • SIP-I • SIP-T • H.323 VoIP Media Transcoding Support • G711u/a • G.729 • G723.1 • G726 • T.38, • AMR/AMR-WB • GSM-FR • GSM-EFR, • Silk • Opus • EVRC-A/-B • EVRC-NW2K Encryption • SIP TLS • SRTP • ZRTP VoIP Proxy

	• Signaling Proxy
	  o SIGTRAN
	  o H.248
	  o MGCP
	• Media Proxy
	  o Voice
	  o Video
	  o Fax
	  o DTMF
	• Transport Layer
	  o TCP/UDP/TLS/DTLS/WebSocket
	• Media Transport Layer
	  o RTP/SRTP/ICE
	• Voice Transcoding
	  o G711/G729/G723/AMR/Opus/etc.
	• Video Transcoding
	  o VP8/H263/H264

	• RTP Profile o AVP/AVPF/SAVP/SAVPF • Transparency of proprietary SIP headers • Performance • Simultaneous Calls 500 to 30,000 • Calls Per Second (CPS) 600 • Max Subscribers up to 250,000 • RADIUS · RADIUS AAA support · RFC 2138,2139 · Cisco VSA compliant In addition, our solution • Border firewall • VPN • IDS/IPS • Session Border Controller (SBC) • Opening and closing of pinholes • Limiting access to critical components through the use of VLANs • Call admission control • Media transcoding • Signaling protocol normalization and interworking • Network address translation (NAT) • Codec negotiation • Support for QoS and priority markings • Media proxy

Any additional documentation can be inserted here

NGCS 20	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **High-Availability Design** The BCF solution shall be deployed in a manner to achieve 99.999 percent availability. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: NGA 911 understands that the BCF solution shall be deployed in a manner to achieve five 9s (99.999%) availability and will comply. BCF H/A performance is attained in two ways. At the edge the BCF is deployed in a fully redundant manner with support for automatic failover. This ensures five 9s (99.999%) reliability at the network edge. Additionally, NGA 911 has engineered for geo diverse Direct Connect into the Primary and Secondary PSAPs where each connection is meshed with AWS through the AWS Direct Connect Partner Network.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 21	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Auditing of System Log Files** Management of the BCF shall include continuous auditing of the system log files for anomalies, and processes for responding to and managing security incidents. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The BCF/Session Border Control (SBC) is fully integrated into the Network Monitoring System (NMS) utilized by the Network Operations Center (NOC) and monitored by the Security Operations Center (SOC). The BCF is on the front line of our comprehensive Defense in Depth Security Approach. As such ingress rules, B2BUA criteria and all signaling and media traffic are defined, monitored, and authenticated via TLS. Additionally, we continuously monitor, test, and measure performance utilizing Darktraces' AI technology. Management of the BCF includes auditing of system log files for anomalies and processes for responding to and managing security incidents. We have established an information program with designated roles and responsibilities that are appropriately aligned within the organization. Our management reviews and evaluates the risks identified in the risk management program at least annually. The risk management program encompasses the following phases: Identify – The identification phase includes listing out risks (threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities. Assess – The assessment phase considers the potential impact(s) of identified risks to the business and its likelihood of occurrence and includes an evaluation of internal control effectiveness. Mitigate – The mitigate phase includes putting controls, processes and other physical and virtual safeguards in place to prevent and detect identified and assessed risks. Report – The report phase results in risk reports provided to managers with the data they need to make effective business decisions and to comply with internal policies and applicable regulations. Monitor – The monitor phase includes NGA 911 Compliance performing monitoring activities to evaluate whether processes, initiatives, functions and/or activities are mitigating the risk as designed. Our management leads an information security program that identifies and establishes security goals that are relevant to business requirements. Annual evaluations are performed to allocate the resources necessary for performing information security activities to meet or exceed customer and service specifications.				

Any additional documentation can be inserted here

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 22	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Silence Suppression Detection** The BCF shall be capable of detecting when silence suppression is present in the 911 call and of disabling silence suppression if it is detected in the call. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The NGA 911 BCF is capable of detecting when silence suppression is present in the 911 call and disabling it. If it is detected in the call, our BCF will inject 'comfort' noise that is associated with an open session for which a BYE or other message or indication for call termination has not been received.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 23	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **SIP Call Mediation** The BCF shall mediate all incoming 911 calls from VoIP providers to Session Initiation Protocol (SIP) calls and should be done in accordance with NENA-STA-010.2-2016. Any specific variations or non-compliance with this requirement shall be identified and documented below. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The NGA 911 BCF mediates incoming calls from VoIP providers that are not already processed by the VPC (VoIP Positioning Center) and formatted for SIP i3 in accordance with NENA-STA-010.2-2016. This is the case where VoIP bypasses the VPC deployed by NGA 911 and is not native i3 compliant. Our BCF supports Back-to-Back User Agents (B2BUAs) for SIP and thus enables ESRP interworking across ESInets. NGA 911 has no specific variations or non-compliance to report.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 24	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Event Logging** The BCF shall provide the functionality to maintain logs of all 911 sessions and all additional BCF logging and recording requirements, as specified in NENA-STA-010.2-2016. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: Both of the major elements in NGA 911's BCF solution, the Firewall and the SBC utilize the ESInet logging services to log all significant 911 call flow milestones in compliance with the specification in NENA-STA-010.2-2016. In addition to logging these call flow events, both elements also log additional significant security and administrative information which is used by our NOC/SOC to help evaluate and adjust the performance of the ESInet. The BCF provides the functionality to maintain logs of all 9-1-1 sessions and all additional BCF logging and recording requirements, which are maintained by the NGA 911 MIS.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 25	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **NAT/NAPT Detection and Mediation** Provide details on how the proposed Session Border Control (SBC) will recognize that a Network Address Translation (NAT) or Network Address and Port Translation (NAPT) has been performed on Open Systems Interconnection (OSI) Layer 3, but not above, and correct the signaling message for SIP.	X			
	Bidder Response: The NGA 911 solutions Session Border Control recognizes that a NAT or network address and port translation (NAPT) has been performed on Open Systems Interconnection (OSI) Layer 3 and correct the signaling message for SIP by the following: The NGA 911 SBC is configured to recognize and perform NAPT operations in support of implementing a Topology-Hiding Inter-network Gateway (THIG) sub-function. This sub-function performs signaling-based topology hiding, IPv4-IPv6 interworking and session screening based upon source and destination signaling addresses. It also utilizes an inter-working function when connecting non-SIP or non-IPv6 networks. It also interacts with the transport boundary at layers 3 and 4 for control of the boundary at the transport layers including pinhole firewall, Network Address and Port Translations (NAPT) and numerous other features. THIG also restores the headers IP addresses when NATing back to the original network.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 26	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **IPv4/IPv6 Interworking** Provide details on how the proposed SBC shall enable interworking between networks utilizing IPv4 and IPv6 through the use of dual stacks, selectable for each SBC interface, based on NENA-STA-010.2-2016. All valid IPv4 addresses and parameters shall be translated to/from the equivalent IPv6 values.	X			
	Bidder Response: The NGA 911 solution is the most effective and efficient IP routing solution. All NGA 911 servers, systems, routers, switches and other network equipment supplied as part of this contract support dual stacks. The NGA 911 ESInet as a matter of practice and in accordance with the standards accepts and routes IPv4 and IPv6 packets. Each addressable service also supports IPv4 and IPv6 interfaces. IPv6 is recommended for use throughout the ESInet, but cannot be assumed based on the capabilities and limitations of equipment, functions and services that are authorized and credentialed to interact with the ESInet. In such cases the default addressing scheme will be IPv4 through the provisioning of IPv4/IPv6 Interworking at the BCF. IPv4/IPv6 Interworking: The Session Border Control (SBC) component of the Border Control Function (BCF) enables interworking between networks utilizing IPv4 and networks using IPv6 through the use of dual stacks, selectable for each SBC interface. All valid IPv4 addresses and parameters will be translated to/from the equivalent IPv6 values. There should not be any errors as the result of running a dual stack environment. Nonetheless, routers on the network will monitor the dual stack implementation with the ability to fallback to IPv4 if any issues arise.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 27	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **SIP Support Over Multiple Protocols** Provide details on how the proposed SBC shall support SIP over the following protocols: 1. Transmission Control Protocol (TCP), 2. User Datagram Protocol (UDP), 3. Transport Layer Security over TCP (TLS-over-TCP), and 4. Stream Control Transmission Protocol (SCTP). Protocols supported shall be selectable for each SBC interface to external systems. These transport layer protocols are generated and terminated at each interface to external systems.	X			
	Bidder Response: The NGA 911 SBC Appliance (based on Kamailio Modules) support SIP over the following protocols: Transmission Control Protocol ("TCP"), User Datagram Protocol ("UDP"), Transport Layer Security ("TLS") over TCP, and Stream Control Transmission Protocol ("SCTP"). These protocols are selectable for each SBC interface to external systems where they are "negotiated" during the initial INVITE directly or as part of a B2BUA. These transport layer protocols are generated and terminated at each interface to external systems. The SBC applies firewall rules associated with addresses, ports, services and sessions, access control lists ("ACLs"), and establishes virtual local area networks ("VLANs") and virtual private networks ("VPNs") for PSAP client and customer data security. TLS/SSL and TLS with AES protocols are used to control network traffic and access. The Certificate Authority (CA) necessary for the issuance and validation of TLS certificates will need to be shared and accepted between the parties. Until the PSAP Credentialing Agency (PCA) is established, NGA 911 will work bilaterally with all potential call "presenters" to facilitate strictly secure and authenticated access to the State of Nebraska ESInet/NGCS for the purposes of 9-1-1 call delivery.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 28	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Packet Prioritization Based on Session Type** Provide details on how the proposed SBC shall be capable of populating the Layer 3 headers, based on call/session type (e.g., 911 calls) in order to facilitate priority routing of the packets.	X			

Bidder Response:

The NGA 911 SBC is capable of packet prioritization which are routed through the population of DSCP codes received in SIP, based on call/session type (e.g., 9-1-1 calls) in order to facilitate priority routing of the packets. The NGA 911 SBC enforces DiffServ (RFC 2474) code points DSCP to differentiate traffic throughout the Ingress Network. The SBC is fully state-aware at layer 2 through 7. SBCs implement a SIP back-to-back user agent (B2BUA) as defined in IETF RFC 3261. A B2BUA divides each SIP session into two distinct segments, as shown in the following diagram. In doing so, the SBC is able to completely and effectively control SIP sessions, as well as the associated media flows, in ways that SIP ALGs cannot. This unique capability gives SBCs a clear edge in their ability to securely deliver reliable, high-quality, IP-based interactive communications. All routing elements related to Media and Session anchoring in the ESInet and including the SBC honor the DS Field code point and Per Hop Behavior (PHB) in compliance with NENA:

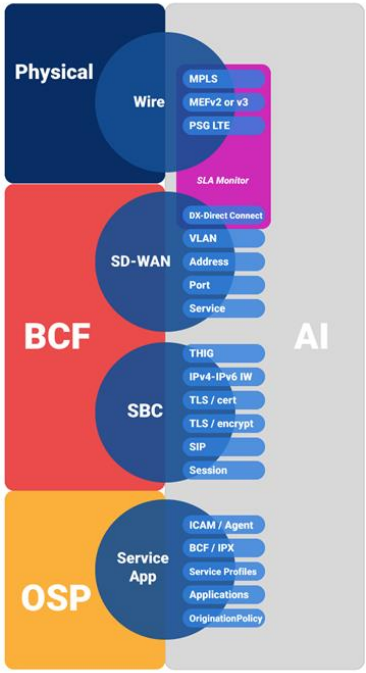
DSCP	Use	PHB
1	Routine Traffic	Default
5	9-1-1 Signaling	AF12
9	9-1-1 Text Media	AF12
13	9-1-1 Audio Media	EF
17	9-1-1 Video Media	AF11
21	9-1-1 Non-human-initiated Call	AF21
25	Intra ESInet Events	AF21
29	Intra ESInet Other 9-1-1 Traffic	AF22

Any additional documentation can be inserted here:

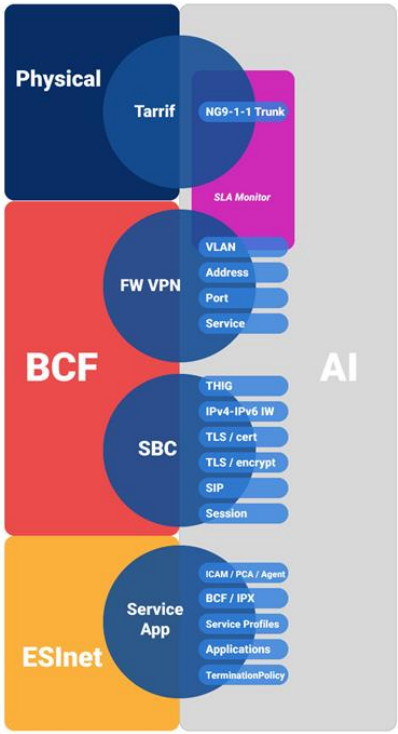
		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 29	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **Encryption of Unencrypted Calls** Provide details on how the proposed SBC supports encryption for calls that are not protected entering the ESInet, based on NENA-STA-010.2-2016.	X			
	Bidder Response: Calls going across the ESInet, whether they start as encrypted or not, are carried using TLS which encrypts the call after it hits the SBC through to its endpoint based on NENA-SYA-010.2-2016.				

Any additional documentation can be inserted here:

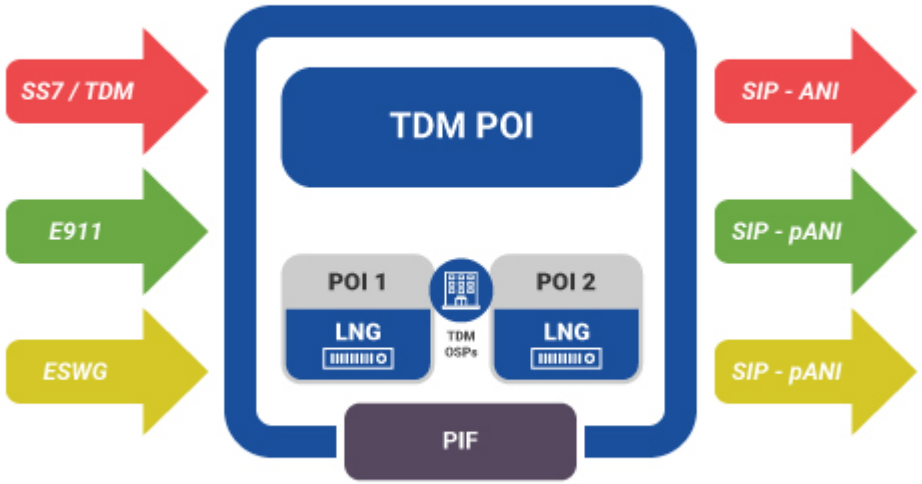
		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 30	**Next Generation Core Services Elements (NGCS)** **Border Control Function (BCF)** **BCF Elements** 1. Provide details, including drawings, describing the different BCF elements that the proposed solution comprises. 2. As part of the details, identify all of the elements and/or interfaces to be provided by the Commission and/or PSAPs to the bidder.	X			
	Bidder Response: The BCF element of NGA 911's solution interfaces the NGCS to the outside world. The NGA 911 solution includes the incorporation and use of BCF as appropriate with security devices implemented in the ESInet and at the "edge" of the ESInet where it meets OSPs, CPEs, other ESInets or Non-NG networks either directly or through LNGs and LPGs. The physical location or the virtual implementation of the BCFs are dependent on the equipment and capabilities of interfacing partners. NGA supplies i3 compliant or custom interfacing options (for non-compliant providers) as follows: a. OSP - BCF ○ i. Direct Cloud Interface (Peering or Transit Gateway) ○ ii. Cross Connect Interface (IXC) ○ iii. Direct Physical Interface				



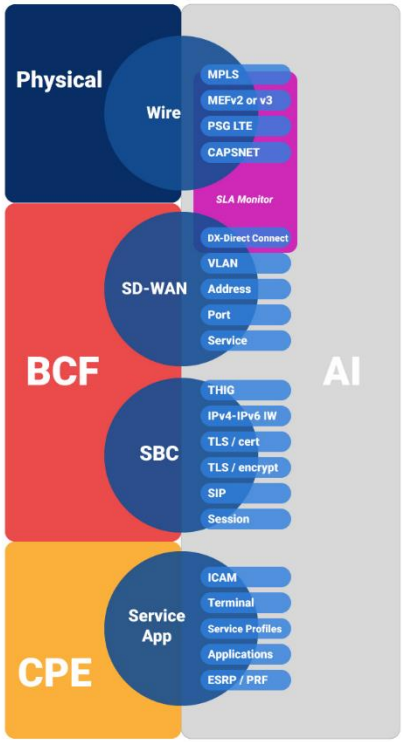
b. Other ESInets
- i. Direct Cloud Interface (Peering or Transit Gateway)
- ii. Cross Connect Interface (IXC)
- iii. Direct Physical Interface



c. Non-NG Networks
- i. TDM Gateway (PSTN)
- ii. Media Gateway
- iii. SS7/SIGTRAN
- iv. Cross Connect Interface (IXC)
- v. Direct Physical Interface



d. PSAPs
- i. Physical Connection with PSAP FW (VPN)
- ii. Virtual Connection with PSAP BCF
- iii. Provisioning of BCF for non-compliant PSAPs offered by NGA 911



NGA 911 will require Nebraska to provide information on the types of physical interfaces to the ESInet they can provide at each location they want to interface with the ESInet. Based on the information we would expect that to be at each of the 11 regional PSAP host locations in Nebraska referenced in Attachment A of this RFP.

NGA 911 utilizes carrier class Border Control Function (BCF) to provide a uniform network interface with comprehensive security features when linking between Next Generation Network Domains including VoIP, SIP, HTTPS interfaces and VoLTE / IMS networks. Network signaling and media settings are deployed through a comprehensive OA&M web-based interface. The BCF exceeds all functions listed above and the requirements described in NENA 08-003 (superseded by NENA STA-010.2-2016 and soon STA-010.3), as well as additional firewall requirements described in NENA 04-503 and NENA 75-001 (NG-SEC).

	The BCF is the interface of two disparate networks that negotiate, limit, regulate, and secure traffic based on authentication, authorization, traffic type, ports, address-translation, QoS, and session. In i3 the BCF provides border functionality between the Ingress Aggregation Network, other ESInets, member PSAPs, permitted foreign functional elements such as ESRP's, LIS's, and authorized API's for the purposes of report querying. Ideally all interactions with the BCF are secured by credentials issued by the PCA; but as of yet the PCA has not been established; so, all BCF to BCF interfaces will be bilaterally negotiated and credentialed by mutual agreement in the meantime. The NGA 911 BCF functionality addresses the requirements at the boundary where different service provider or peer networks interconnect to the NGCS. The NGA 911 BCF provides security for your NGCS in terms of signaling information by implementing a Topology-Hiding Inter-network Gateway (THIG) sub-function. This sub-function performs signaling-based topology hiding, IPv4-IPv6 interworking and session screening based upon source and destination signaling addresses. It also utilizes an inter-working function when connecting non-SIP or non-IPv6 networks. It also interacts with the transport boundary at layers 3 and 4 for control of the boundary at the transport layers including pinhole firewall, Network Address and Port Translations (NAPT) and numerous other features. Quality of service (QoS) packet marking, bandwidth policing, usage metering and QoS measurements for the media flows are additional features supported by the BCF. The NGA 911 solution does not require physical equipment/hardware. The BCF is implemented as a Virtual Network Function (VNF) Appliance in the Amazon Web Service (AWS). A critical function of the BCF is to secure the ESInet. The NGA 911 network runs an Intrusion Prevention System (IPS) capability within the Border Control Function (BCF) network firewall to monitor and evaluate network traffic to detect and prevent network threats from entering the NGCS. The IPS is integrated with the network gateway to provide the ability to apply IPS signatures to Internet Protocol (IP) packets within the GPRS Tunneling Protocol (GTP) User (GTP-U) plane tunnels and GTP Control plane (GTP-C) tunnels. The IPS will intercept packets and inspect traffic for various threats (such as signaling storms). This allows for an automatic pass/drop packet decision, plus enables the Security Operation Center (SOC) to monitor and log any malicious events. The IPS also uses unique traffic-learning algorithms to effectively detect network anomalies and block traffic outside of configured thresholds. This effectively stops Distributed Denial of Service (DDoS) attacks and other threats characterized by anomalous traffic patterns. There is also built-in signaling support for Session Initiation Protocol (SIP) to protect voice, text, and media infrastructure and RTP traffic. NGA 911 uses state of the art Cyber Intrusion technology to track possible attacks and unauthorized access while implementing IPSec (3GP TS 33.210) protocols to protect 9-1-1 traffic between the NGCS and the PSAP sites. IPSec will utilize IKE V2 and PKI for peer authentication. BCFs will be used between the state infrastructure and outside networks to secure data on potentially untrusted networks for network domain security. Inter Core element signaling will be protected across the transport networking utilizing Group Domain of Interpretation (GDOI) VPNs and site-to-site VPNs, as appropriate. Advanced Encryption Standard (AES) 128/256 encryption will be available over interconnection network on both fiber and microwave links to ensure all traffic is secure from outside monitoring. Firewalls will be used to protect all interfaces to ESInet against TCP sweeps, denial of service attacks (i.e., bandwidth saturation attacks), botnet attacks, and IPv6-related DDOS attacks, among other of the ever-increasing threats against mobile networks.

	A key component of our Host Layer Defense in Depth Security posture has a number of features and functions for avoiding, minimizing, and limiting malicious activity that may occur at any point within the NGA 911 ESInet and NGCS system. The focus of malicious activity is on Core Security which is built upon the following elements. o Server Hardening o ESInet Based Firewall o Virus Protection o Intrusion Prevention o Patch Management Server hardening involves making sure our OS is hardened which in large part is handled through the use of customer Docker Containers. Access to the containers is strictly managed through our IAM. ESInet based firewalls are covered by the comprehensive application of the inherent BCF/SBC/FW functions and elements we built into the ESInet in accordance with the specifications. Virus protection is covered by subscriptions (managed by the SOC) to several leading Anti-Virus software providers. Intrusion prevention in addition to intrusion protection detailed below is managed through Artificial Intelligence - AI (the details are subject to confidentiality protections and a need to know basis) that quickly identifies, monitors, and reports anomalies that might be the result of a day-zero attack. And finally, this is all managed by our SOC processes and procedures as detailed and maintained in our SPN.

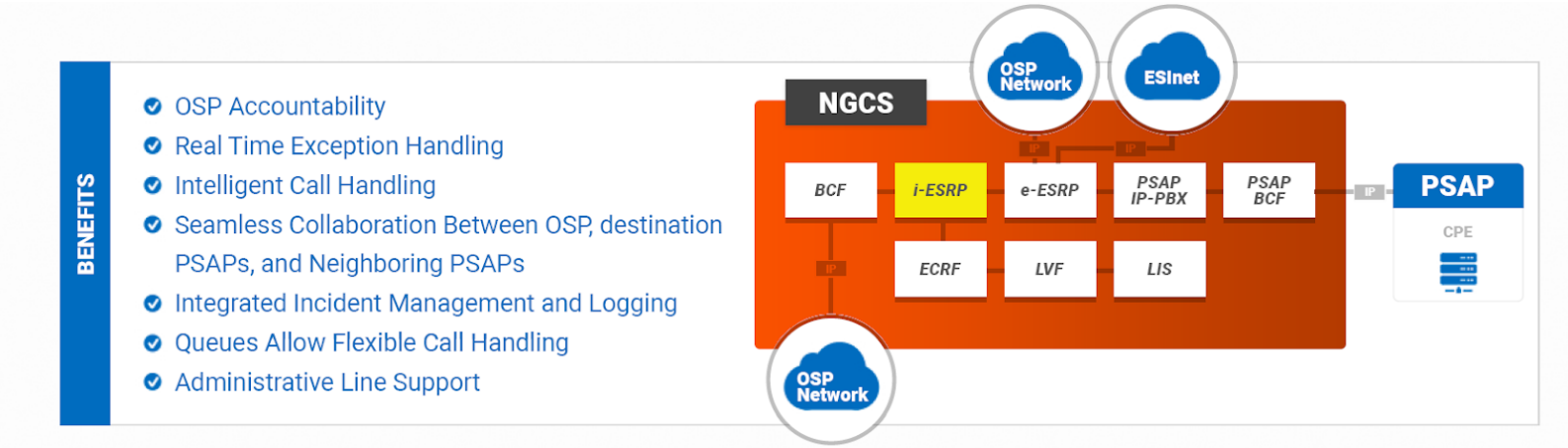
Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 31	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **ESRP Description** The ESRP routes a call to the next hop. It also evaluates the originating policy rules set for the queue the call arrives on, extracts the location of the caller from the SIP signaling, queries the Emergency Call Routing Function (ECRF) for the nominal next-hop route, evaluates the route based on policy rules and queue states of the downstream entity queues, and then forwards the call to the resulting next hop. Bidder's proposed ESRP must meet or exceed NENA-STA-010.2-2016. Describe how the proposed solution meets or exceeds the standards.	X			

Bidder Response:

As per the NENA Architecture

- The "Originating ESRP" is the first routing element inside the NGCS. It receives calls from the BCF at the edge of the NGCS
- One or more "Intermediate ESRPs" which exist at various hierarchical levels in the NGCS. For example, the Originating ESRP may be a state-level function, and an intermediate ESRP may be operated by a county agency;
- The "Terminating ESRP" is typically at the edge of the NGCS, just before the PSAP BCF.



Originating and Terminating ESRP's.

The Originating ESRP is responsible for managing the rules and policies governing the interaction between the OSP networks and NGCS as well as extracting location information from the call and routing to the Terminating ESRP with appropriate location information.

	The Terminating ESRP is responsible managing the policies governing PSAP's operating status and protocols with inbound 9-1-1 calls. The NGA 911 ESRP is instantiated as virtual instances within AWS Virtual Private Clouds (VPCs) hosted in separate availability zones (AZs) and Regions. As a distributed deployment simultaneously handling redundant traffic flows ensures reliability and supports resiliency. The NGA 911 ESRP is configured according to NENA STA-010 specifications. Legacy incoming calls are routed from LNGs and Native i3 SIP signaling is forwarded from the BCF to the corresponding ESRP. The ESRP evaluates the location for the nominal next-hop route queue whether that is another ESRP, call relay system, LRSG or NG9-1-1 PSAP. The ESRP interfaces to the ECRF and to the PRF to ensure that routing instructions, routing policies and possible event notifications that alter call routing scenarios are acknowledged. In accordance with NENA STA-010.2-2016 for typical 9-1-1 calls received the NGA 911 ESRP: 1. Evaluates a policy "rule set" for the queue the call arrives on 2. Queries the location-based routing function (ECRF) with the location included with the call to determine the "normal" next hop (smaller political or network subdivision, PSAP or call taker group) URI. 3. Evaluate the policy rule set for that URI using other inputs available to it such as headers in the SIP message, time of day, PSAP state, etc. The result of the policy rule evaluation is a Uniform Resource Identifier (URI). The ESRP forwards the call to the URI. The NGA 911 ESRP supports SIP SUBSCRIBE/NOTIFY in order to understand the status of both upstream and downstream elements. In the event that the call is unable to be delivered to a PSAP via the ESInet, the LSRG that is provided as part of this contract will be used to transfer the call to a legacy PSAP. NGA 911 can also provide an alternate option: a 3GPP IP Multimedia Subsystem (IMS). An IMS functions as a gateway between IP and the PSTN as a gateway.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 32	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **Transition to Geospatial Routing** Bidder understands that all PSAPs and regions may not be ready for geospatial routing on day one of operations and shall provide tabular routing services, also known as Internet Protocol Selective Routing (IPSR), until such time as PSAPs and regions are ready for geospatial routing. In bidder's separate cost proposal response, indicate the pricing difference between tabular and geospatial routing. Describe the process for transitioning each PSAP or region from tabular routing to geospatial routing as PSAP's becomes ready and the manner in which the solution provides for routing by both means simultaneously.	X			
	Bidder Response: NGA 911 will handle both tabular and geospatial routing. NGA 911 is offering Nebraska it's cloud-hosted LDB product as a transitional element to a LIS. The NGA 911 LDB serves as both a legacy ALI database and as a LIS in an i3 NG9-1-1 environment. The LDB will retain all of the current information, functionality, and interfaces of today's ALI, but also can use the new protocols required in an NG9-1-1 deployment. The LDB supports the protocols for legacy ALI query and ALI query service, the protocols required to obtain information for wireless calls by querying the mobile positioning center (MPC) or gateway mobile location center (GMLC), and the protocols required for i3 location information retrieval and conveyance, such as HELD or other proprietary protocols. As Nebraska transitions to a full NG Core, this element in conjunction with the LVF to validate addresses from either legacy MSAG formatted locations or i3 based PIDF-LO formatted ones. The LDB is available to Originating Service Providers (OSPs) so they can verify that civic addresses will return PSAP or emergency responder URIs either using an Application Program Interface (API) Gateway or through an NGA 911 provided web-based solution from our partner COMsolve. The choice of which method used is determined by the needs and requirements of the OSP. The LDB/LIS we are providing serves civic addresses and includes support for E911 and i2 as well. These additional features enhance ingress routing for all legacy providers, wireline, wireless and VoIP. For this reason, our LDB/LIS maintenance and support interface provides for not only the verification of civic addresses, but also ESRK, ESRD (pANI) for E9-1-1, and ESQK for i2. In preparing the LDB as the routing database for legacy OSPs, locations and keys will initially be ingested in bulk and verified against a data dump from the existing legacy ALI/MSAG/SRDB. Given the diverse sources of this information these loads will not necessarily all be completed at one time. Different parties will be required to verify the data sets relevant for their client records including OSPs, MPC/GMLC's VPC, and other location key and data providers. Verification will depend on the type of service provided whether it is an actual civic address, or a key range. Civic addresses and key ranges are associated with PSAP routing boundaries in the GIS and				

updated in the LVF validation data prior to being active in the LDB. The process is complete when an input from an OSP or Location Service Provider regularly and uniquely returns the correct emergency responder URI associated with a PSAP endpoint.

After initial loading, verification and validation, the LDB must be regularly updated by the OSPs and Location Service Providers. NGA 911 offers a number of different options for the LECs to manage their Service Order Input (SOI) Updates. Proper updating requires adherence to a process to ensure data is ingested and the LDB integrity is protected. The OSP sends data to NGA 911 by one of the available ingest methods. The SOI files are loaded into the NGA 911 COMsolve system for processing. The SOI updates validate against the different databases and tables depending on the source and LDB category of the input, if a record passes all validations, the update is applied to the LDB. If the record does not successfully pass all required validations, an error is returned with error codes associated with the specific error type and the update is not applied to the LDB until the error is resolved.

The COMsolve Web input system automates either single site or batch of the following operations and activities:

- Civic Address management (SOI) features include add civic address, validate address is resolvable in GIS, update the LVF and activate in the LDB
- ESRK/ESRD management features include add ESRK/ESRD range, for ESRD implementations, allocate ESRDs to cell tower, for ESRK implementations - link ESRK range to PSAP and allocate cell tower to appropriate ESRK range, monitor ESRKs/ESRDs level, and warn when ESRK/ESRD levels are low
- 9-1-1 routing table import updates to routing tables, determine required changes, reassign ESRK Ranges/ESRDs, determine if new 911 trunks are needed, generate LDB list load files to include local address verification function (LVF) pre-check against GIS database where results are made available to OSP, and can be used to update LDB for fixed line applications (ports, adds, disconnects).

Utilizing AWS Lambda API Gateway, the LDB loading and query verification service is available 24x7x365 for authorized OSPs and users to upload, verify and validate their loads. The Lambda microservice APIs act as a "front door" for OSP civic address verification. This service handles hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management.

	It is vital that NGA 911's LDB be accessible by Originating Service Providers (OSPs) and other authorized users so they can verify that civic addresses will return PSAP or emergency responder URIs. Without this capability OSPs and Nebraska's dialing 9-1-1 would face unacceptable delays in emergency response due to misrouting and the subsequent transfer between authoritative agencies.

Any additional documentation can be inserted here:

NGCS 33	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **Policy Routing Function (PRF) Description** The PRF is a required function of the ESRP. The ESRP interacts with the PRF to determine the next hop of a call or event. Before the ESRP sends the call to the next hop, it first queries the PRF to check the status of the next hop to determine if a unique routing rule or policy is in place that would direct the call to another location. The destination of the next hop is typically a queue. The PRF monitors the downstream queues of ESRPs for active understanding of the entity's queue status. Describe how the solution meets or exceeds the standards.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The NGA 911 Policy Routing Function (PRF) is the primary routing component of the ESRP. The ESRP uses defined routing policies within the ESInet and the NENA i3 network to deliver calls to the call-takers. The PRF provides the information to the ESRP in order to dynamically route and re-route calls based upon policies and rules that must be implemented beyond normal operations. The PRF monitors the downstream queues of ESRPs to actively understand each potential entity's queue status. The PRF functionality supports both default and alternate routing, and tabular routing for calls arriving without accurate location data.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 34	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **PRF Policy Store and User Interface** The PRF shall allow defining of policy rules for distributing a wide range of calls in an efficient manner. 1. Describe the solution's Policy Store and the PSAP's ability to effect changes to the PRF. 2. Describe the user interface, role-based authentication, the ability of each PSAP or region to manage PSAP's own policy rules, and the types of policy rules available at the time of proposal submission, as well as those on the product roadmap. Roadmap items must include an estimated time of feature availability.	X			
	Bidder Response: The PSAP or region can manage their policy rules through NGA 911's Web-based Portal. NGA 911 supports all current defined PRR including pre planned or ad hoc. If a PSAP cannot access the portal they can call the NOC and, with proper authentication, activate either type of PRR. In accordance with the i3 Standard, NGA 911 will use the following method of call routing using the Policy Routing Function (PRF). The PRF is served by the Policy Store, which will hold OriginatingPolicy(ies) and TerminatingPolicy(ies) in Policy Rulesets, with each Policy Rule Set containing the applicable Policy Routing Rules (PRR). NGA 911's solution has the capabilities for direct PSAP activation and deactivation of predefined alternate routing policies. Below is a description of how a call would be affected in its path by PSAP's predefined policies and what the PSAP would use to activate/deactivate PRR: 1. After a call is pre-processed by the NGA 911 Aggregation Services, it arrives through the BCF at the serving ESRP. 2. The ESRP takes the available information from the SIP Header (the content of the Header fields will be dependent on call type: i3, i2, E911, Legacy – TN) and sends the URN and location information to the ECRF. The ECRF returns the "Normal-NextHop" URI. 3. The ESRP presents the "Normal-NextHop" URI to the PRF, which checks it against the current "Route Policy" from the Policy Store for that URI and executes the ruleset. The ruleset provides the ESRP with the actual destination URI. 4. The PRF also has access to the queue state of downstream entities, which it uses when evaluating the rulesets to determine the destination URI. 5. Generally, the 'next hop' (destination URI) will be one of three types: most often a 'final hop' to the serving PSAP in the domain of the ESRP, a 'final hop' to a secondary PSAP that is handling the serving PSAPs call or calls due to settings in the serving PSAP's PRF, or the 'next hop' to another ESRP most likely in another domain. 6. The Policy Routing Rules will be developed in consultation with the PSAP and State of Nebraska. It is expected that these rules will be based on the existing alternate routing instructions provided by the legacy Selective Router programming today, but routing capabilities are no longer restricted by SR connectivity, so calls may be routed to any PSAP reachable through an ESInet.				

	7. It is expected that the PSAP(s) will have mutual aid agreements in place to effect diversion of calls using the PRRs. 8. PRRs will be tested to ensure no conflicts exist in accordance with v3 of the i3 Standard (forthcoming) using the purpose parameter of "emergency-prr-test" in the Call-Info header field. 9. The capability to invoke or revoke (activate or deactivate) predefined alternate routing policies is provided in the PSAP Dashboard. We also provide an ad hoc interface to the PRF for alternate routing of calls in the event of an emergency condition affecting one or more PSAPs. For ad hoc situations, such as an emergency impacting a particular area, a Policy Rule is created in conjunction with the ad hoc creation of a GIS polygon describing the affected area. Since the SI updates the ECRF in near real-time, any changes to GIS will take effect almost immediately. This allows the PSAP to modify the destination Queue Identifier for an established polygon or to create a new polygon with a discrete Queue to specify a different call treatment. For example, a crash on the interstate typically creates a spike in call volume, which may impair other emergency calls from reaching a call taker. An authorized individual can inscribe a polygon around the crash site with all calls within the polygon directed to a specific position within the PSAP for answering, to a different PSAP, or an Interactive Media Response (IMR) System if available. Alternatively, a Policy Routing Rule could be constructed and invoked to affect the same result. In the case of a ransomware attack on a CHE system serving multiple PSAPs, an ad hoc Policy Rule will be created by the NGA 911 support staff to immediately redirect calls under this debilitating condition. The NGA 911 support staff monitors the system 24x7x365 to identify these types of attacks and respond accordingly.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 35	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **Next-Hop Queues** A next-hop queue may be a Uniform Resource Identifier (URI) that routes the call to an interactive multimedia response system (as described in IETF RFC 4240) that plays an announcement (in the media negotiated by the caller) and potentially accepts responses via Dual-Tone Multi-Frequency (DTMF) signaling or other interaction protocols. Describe how the bidder's solution implements next-hop queueing.	X			
	Bidder Response: The NGA 911 NGCS solution includes a fully NENA i3 compliant PRF that can alter the routing of calls in conjunction with the ESRP based on the queue status of the next-hop. NGA 911 fully supports DTMF in the ESRP. The NGCS ESRP will route SIP signaling and a media path between the interactive media response system and the caller which is capable of supporting DTMF responses.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 36	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **High-Availability Design** The ESRP/PRF solution shall be designed with resiliency and redundancy to provide a minimum of 99.999 percent availability. Describe how the solution meets or exceeds the above requirements.	X			

Bidder Response:

NGA 911's NGCS (including the ESRP/PRF) is 100% deployed in the cloud, providing the best possible reliability and availability in the industry. All functional elements (FE) of the NGA 911 NGCS are designed, architected, and deployed on the AWS Cloud in a manner which strictly adheres to the criteria defined in NENA-STA-010.2-2016 for an NGCS.

All Amazon Web Services (AWS) data centers and direct connect facilities are designed to an Uptime Institute level of Tier III+ or above. The NGA 911 solution is fully redundant, deploys dual Cores in four (4) Availability Zones (AZ) for a total of eight (8) Cores. The AWS AZs are required to be a minimum of 10 miles apart and on separate power grids. The AZs are connected by multiple high-speed broadband carriers in meshed networks. Having 8 cores allows NGA 911 to exceed Nebraska's five 9s availability requirement.

NGCS	Non Redundant 1 AZ		Redundant 2 AZ		Redundant Region 2 AZ's each	
Functional Element	Signaling	Media	Signaling	Media	Signaling	Media
Aggregation Point	99.90%	99.95%	= 5 9's	> 5 9's	100.00%	100.00%
NG911 Trunk	99.99%	99.99%	> 5 9's	> 5 9's	100.00%	100.00%
BCF	99.99%	99.99%	> 5 9's	> 5 9's	100.00%	100.00%
NGCS	99.84%	99.95%	> 5 9's	> 5 9's	100.00%	100.00%
BCF	99.99%	99.99%	> 5 9's	> 5 9's	100.00%	100.00%
NG911 Trunk	99.99%	99.99%	> 5 9's	> 5 9's	100.00%	100.00%

**100% signifies many 9's above five 9's*

Each of the 8 NGCS cores are architected to support 100% of the traffic for Nebraska. The NGA 911 cores operate in an active-active mode. SIP Signaling is processed through the eight (8) cores dedicated to Nebraska utilizing a load balancing round robin approach that ensures all network FE's are constantly and consistently exercised. In the event of failure of any one stack, that supporting core infrastructure is taken offline and replaced with a new container of the instance without effect to the other operational cores. This

approach ensures that there is never a gap in availability and exceeds the five 9s requirements defined by Nebraska. 100% of the platform capacity will survive any single element of the solution experiencing a failure.

The NGA 911 NGCS meets the following characteristics:

Reliability: probability of uptime of each component under normal conditions is designed to exceed five 9s (99.999%).

Availability: probability of uptime of a system under normal conditions is designed to exceed five 9s (99.999%).

End-to-end Availability (non-redundant): probability that all components in the system, in this case the eNodeB, transport and core, are functioning, not considering redundant or overlapping coverage is designed to e

Resiliency: the ability of a system to continue to operate during or recover after a disaster.

Redundancy: the duplication of components in a system (improves reliability and availability and can be a form of resiliency).

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 37	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF)** **Keep-Alive Signaling Between Elements** Provide an explanation of how the proposed ESRPs use the SIP "options" transactions for maintaining "keep -alive" signaling between ESRPs, LNGs, Legacy PSAP Gateways (LPGs) and session recording services.	X			
	Bidder Response: The NGA 911 ESRP solution implements "options" as defined in RFC 3261 as a "keep alive" mechanism. As the upstream element the ESRP is the initiator of "options" and during periods of inactivity, it will periodically send "options" toward its downstream entities such as other ESRPs, LNGs, LPGs and other SIP based entities in a stream. The period between "options" requests used for keep-alive is provisioned, and default to one (1) minute (which must be less than the Transport Layer Security (TLS) timeout period) intervals during periods of inactivity.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 38	**Next Generation Core Services Elements (NGCS)** **Emergency Service Routing Proxy (ESRP) and Policy Routing Function (PRF** **TCP/TLS Implementation** The upstream interface on the proposed non-originating ESRPs shall implement Transmission Control Protocol/Transmission Layer Security (TCP/TLS), but shall be capable of fallback to UDP, as described in NENA-STA-010.2-2016. Stream Control Transmission Protocol (SCTP) support is optional. The ESRP shall maintain persistent TCP and TLS connections to the downstream ESRPs or User Agents (UA) that it serves. Provide detailed documentation describing how the non-originating ESRP interface supports TCP/TLS with fallback to UDP.	X			
	Bidder Response: The NGA 911 ESRP is designed to handle any type of SIP Header whether conforming to NENA i3 or not. As long as the Header can be parsed and the most rudimentary SIP call information obtained such as origin, destination, and codec the call will be routed (even if to a default or fallback number). Even a malformed call is considered privileged and a default emergency call since the ESRP has an upstream SIP interface that typically faces a BCF for the originating ESRP or an upstream ESRP for an intermediate or terminating ESRP. Such an interface implies that the call is coming from a "trusted" source. This interface also is used by a PSAP, or a BCF between a PSAP and the ESRP for calls sent by the PSAP, but in that case it is expected to be more likely to be with a compliant Header. The upstream SIP call interface for the originating ESRP only assumes the minimal methods and headers and will handle any valid SIP transaction. The ESRP must respond to the URI returned by the ECRF and/or specified in a Route action for a rule for the upstream service the ESRP receives calls from for calls sent to "urn:service:sos". The upstream interface on the non-originating ESRP implements TCP/TLS but is capable of fallback to UDP (as described in NENA-STA-0101.2-2016). SCTP support is optional. The ESRP should maintain persistent TCP and TLS connections to downstream ESRPs or UAs that it serves. If the non-originating ESRP is in another ESInet and prior to the establishment of the PCA, TCP/TLS will only be supported by the third party credentialled agent (certificates) mutually agreed to by the parties.				

Any additional documentation can be inserted here:

NGCS 39	**Next Generation Core Services Elements (NGCS)** **NENA Compliance Chart** Provide a description of how the proposed ESRPs meet or exceed all functional requirements below as defined in NENA-STA-010.2-2016, which are listed below.	X			
	Bidder Response: All of these must-haves from the NENA standards represent the minimal requirements for a compliant ESRP/PRF and NGA 911's solution is compliant with all of them. But what makes NGA 911's solution unique is the cloud implementation which provides an unprecedented availability and reliability which exceeds Nebraska's (and NENA's) requirements.				

Any additional documentation can be inserted here:

	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
Overview Section 5.2.1.1	X			
Call Queueing Section 5.2.1.2	X			
Queue State Event Package Section 5.2.1.3	X			
De-queue Registration Event Package Section 5.2.1.	X			
Policy Routing Function Section 5.2.1.5	X			
ESRP Notify Event Package Section 5.2.1.6	X			
INVITE Transaction Processing Section 5.2.1.7	X			
BYE Transaction Processing Section 5.2.1.8	X			
CANCEL Transaction Processing Section 5.2.1.9	X			
OPTIONS Transaction Processing Section 5.2.1.10	X			
Upstream Call Interface Section 5.2.2.1	X			
Downstream Call Interface Section 5.2.2.2	X			
ECRF Interface Section 5.2.2.3	X			
Location Information Server (LIS) Dereference Interface Section 5.2.2.4	X			
Additional Data Interfaces Section 5.2.2.5	X			
ESRP, PSAP, Call-Taker State Notification and Subscriptions Section 5.2.2.6	X			
Time Interface Section 5.2.2.7	X			
Logging Interface Section 5.2.2.8	X			
Data Structures Section 5.2.3	X			
Policy Elements Section 5.2.4	X			
Provisioning Section 5.2.5	X			

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 40	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** Describe how the ECRF interfaces with other ECRF solutions which may interface with the bidder's solution. Awarded Contractor shall coordinate with other ECRF solution providers to ensure interoperability between the respective solutions.	X			
	Bidder Response: NGA 911 believes that the best architectural approach to implementing ECRF/LVF functionality is to centralize the capability into a single master authoritative ECRF/LVF database. If there are multiple ECRFs either internal or external to the State ESInet that need to interface with master ECRF of Nebraska's NGA 911 supplied Next Generation core they will be supported. NGA 911 will interface with these ECRFs through the LoST interface for queries. For provisioning, these ECRFs, as authorized by the state of Nebraska, will be able "subscribe" to NGA 911's master ECRF/LVF through a provided SI to receive push updates of the latest GIS information from the master. NGA 911 solutions strictly adhere to the NENA-STA-010.2-2016 (originally 08-003) standard and have implemented the interfaces and processes defined in the document to achieve interoperability with ECRFs provided by different vendors. If Nebraska wishes to interface with other vendors' ECRFs that have proprietary or non-compliant interfaces we will write custom middleware to make sure their protocols are translated into proper NENA NG compliant messages.				

Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS) **Emergency Call Routing Function (ECRF)** **ECRF Description** The ECRF shall be designed according to NENA-STA-010.2-2016 and be implemented using diverse, reliable and secure IP connections. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 41		X			

Bidder Response:

The NGA 911 ECRF and LVF fully comply with the requirements delineated in NENA STA-010.2-2016 through the use of a Spatial Interface that consistently applies changes and updates from the statewide GIS through NGA 911's master ECRF/LVF to any subordinate ECRFs either internal or external to the state ESInet. ECRF maintenance is greatly simplified with an ECRF model based on an authoritative ECRF and LVF. The authoritative ECRF and LVF are propagated/replicated to any regional installations in accordance with the processes and schedules developed during the initial setup of the Spatial Interfaces (SI).

Although NGA 911 ECRF can fully function in a tiered hierarchical architecture, NGA 911 believes that a superior approach would be to have one authoritative GIS system and a single master ECRF/LVF to service the entire Nebraska ESInet. This simplified structure is much more conducive to a smooth operational process than trying to manage multiple ECRFs in complex, hierarchical and peer relationships to each other. A single source of the GIS truth is a superior model. Nebraska can provide conditional authority to different jurisdictional agencies to update the parts and layers of the GIS database that they are responsible for but still manage it centrally. The Nebraska ESInet can then provide updates of its information to any external ECRFs that need to subscribe to its data.

NGA 911s Nebraska-wide ECRF and LVF are capable of routing All 9-1-1 traffic within the state. Furthermore, NGA 911 will ensure the following:

- NGA 911 will utilize the statewide GIS database maintained and updated by either the state or us to update the ECRF for routing all 9-1-1 traffic.
- NGA 911's ECRF is capable of receiving updates from the GIS database via our SI, without disruption of ECRF LoST service. Updates shall be at least daily, shall be capable of receiving data updates 24x7x365, and provide confirmation receipt of data within 4 hours.
- NGA 911 provides a process to integrate our maintenance function to upload the data from the statewide GIS dataset to update the ECRF and LVF, ensuring proper routing of calls.

	· NGA 911 will route any 9-1-1 traffic to the appropriate PSAP based on geospatial data and specifically X, Y routing. • NGA 911 provides an Emergency Call Routing Function (ECRF) and Location Validation Functions (LVF) that comply with GIS standards that include but are not limited to NENA STA-010.2-2016 Detailed Functional and Interface Standards for the NENA i3 Solution. Authoritative ECRF and LVF NGA 911's recommendation is that all of Nebraska just use a single ECRF/LVF for all routing and data validation functions. However, if Nebraska chooses to implement a system with unique ECRFs for each region then we recommend that all the regional ECRFs are updated by a single authoritative state ECRF/LVF. Updates to NGA 911's ECRF and LVF occur through the NGA 911-provided SI by Nebraska's sole authoritative GIS database. If this GIS feeds a single master and authoritative ECRF then even if Nebraska should choose to have a regional ECRFs, they would all only have a direct subordinated relationship to the single authoritative master state of Nebraska ECRF. NGA 911 SI processes will ensure that any regional ECRFs (and again we reiterate our recommendation that Nebraska implement only one ECRF for the whole state) or external ECRF/LVF databases are updated and maintained. Alignment of the results when presented with a URN/Location query pair (via the LoST interface) no matter where it is situated in the Nebraska ESInet is the best way to ensure ubiquitous compliance. The recommended flattened hierarchy means that all ECRF and LVFs in the ESInet are based on the authoritative ECRF/ LVF that is validated and updated using the Spatial Interface (SI). ECRF – GIS Updating The NG9-1-1 data management processes ensure updates to the ECRF GIS database are transacted with integrity and do not degrade the performance of the ECRF production system response or disrupt the ECRF LoST service. The NGA 911 team will establish appropriate communication channels and coordination with Nebraska, and any critical third parties to support the update process. The NGA 911 team plans to use a single methodology to control the update processes for both the ECRF/LVF and supporting geospatial datasets from the statewide GIS. The same data should be used for both LVF and ECRF. The system accommodates ad-hoc changes, expedited changes, and a standard planned update process to ensure the most recent and vital information is available to assist callers and first responders. The ESInet Data Management process and supporting technologies are designed and implemented to support multiple types of updates. These updated methods ensure that there is no performance

	degradation to the ECRF LoST services. Updates occur on at least a daily basis unless the update has an effective "on date." Our approach is to work with the statewide GIS service provider and Nebraska to develop a viable and mutually agreeable process that addresses data quality and the specifications for ECRF administration. The ECRF data administration tool uses role-based workflow with the capacity to support staging updates, and coordinates, at a minimum, receiving data updates 24/7/365 and providing a confirmation of receipt of data within 24 hours. Error/DR Change Management To handle records that result in errors or warnings, a governance body review of Discrepancy Reports (DR) would be expected on a weekly basis with the management and technical leads for the respective aspects of the LVF. Our management approaches will accommodate the conditions where critical discrepancies require emergency responses. Our GIS Tools will allow for approved Manual editing as required as well with a set of approved scripts and approval gates which will then use the aforementioned data pipeline process to perform the acquisition, ingestion, validation and augmentation, and ledger recording. The resolution of the discrepancy will be coordinated with the reporting agency and ESInet operational management, and/or appropriate Governance body to align with established change management procedures for data and other configuration items. We assume client governance will allow for resolution based on standing orders as well as escalated items requiring client governance intervention. The team will conform to the emerging NENA standards when finalized and will deploy the best practices of change and configuration management to maintain system integrity and data quality.

Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS) **Emergency Call Routing Function (ECRF)** **High-Availability Design** Bidder shall supply an ECRF function that meets a minimum of 99.999 percent availability. Describe how the solution meets or exceeds the above requirements**.**	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 42		X			

Bidder Response:

NGA 911's NGCS (including the ECRF) is 100% deployed in the cloud, providing the best possible reliability and availability in the industry. All functional elements (FE) of the NGA 911 NGCS are designed, architected, and deployed on the AWS Cloud in a manner which strictly adheres to the criteria defined in NENA-STA-010.2-2016 for an NGCS.

All Amazon Web Services (AWS) data centers and direct connect facilities are designed to an Uptime Institute level of Tier III+ or above. The NGA 911 solution is fully redundant, deploys dual Cores in four (4) Availability Zones (AZ) for a total of eight (8) ECRF instances. The AWS AZs are required to be a minimum of 10 miles apart and on separate power grids. The AZs are connected by multiple high-speed broadband carriers in meshed networks. Having 8 cores allows NGA 911 to exceed Nebraska's five 9s availability requirement. The table below depicts the availability of the key NGCS elements including the ECRF:

NGCS	***Non Redundant 1 AZ***		***Redundant 2 AZ***		***Redundant Region 2 AZ's each***	
Functional Element	**Signaling**	**Media**	**Signaling**	**Media**	**Signaling**	**Media**
AWS Data Element	*99.999%*	*99.999%*	*>99.999%*	*>99.999%*	*100%*	*100%*
BCF	*99.99%*		*>99.999%*		*100%*	
ESRP	*99.95%*	*99.95%*	*>99.999%*	*>99.999%*	*100%*	*100%*
ECRF	*99.95%*		*>99.999%*		*100%*	
LVF	*99.95%*		*>99.999%*		*100%*	
	99.84%	**99.95%**	**>99.999%**	**>99.999%**	**100%**	**100%**

**100% signifies many 9's above five 9's*

	Each of the 8 ECRF are architected to support 100% of the traffic for Nebraska. The NGA 911 cores operate in an active-active mode. SIP Signaling is processed through the eight (8) cores dedicated to Nebraska utilizing a load balancing round robin approach that ensures all network FE's are constantly and consistently exercised. In the event of failure of any one stack, that supporting core infrastructure is taken offline and replaced with a new container of the instance without effect to the other operational cores. This approach ensures that there is never a gap in availability and exceeds the five 9s requirements defined by Nebraska. 100% of the platform capacity will survive any single element of the solution experiencing a failure.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 43	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Accessibility by Outside Functional Elements** Contractors providing an ECRF shall ensure that it is accessible from outside the ESInet and that the ECRF permits querying by an IP client/endpoint, an LNG, an ESRP in a next-generation emergency services network, or by some combination of these functions. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The ECRF can be made available to entities outside the ESInet as long as they are credentialed with the BCF or the yet to be established PCA. The need for an external facing ECRF is dependent on how the Commission wants to route calls at the Ingress. If an external ECRF is required, NGA 911 proposes that there be one inside the ESInet to provide more granular routing (specific PSAP, agency, etc.) after Ingress. We will work with any entity that needs authorized access and provide credentialing accordingly. ECRF/LVFs exist inside and outside the ESInet. Originating networks that route calls to the correct ESInet and validate locations may use external ECRFs. Originating networks may also use equivalent mechanisms that would result in the same route that the external ECRF would provide for the location of the caller for a querier without credentials known by the ECRF. Internal ECRF/LVFs are used by elements inside the ESInet to route calls to the appropriate downstream entity and validate civic locations. While the interfaces and functional descriptions are nearly identical, the provisioning data may not be the same for internal and external ECRFs. An external ECRF need only have the external (which ESInet) route for "urn:service:sos.*" The internal ECRF also needs routes for ESRP use ("urn:nena:service:sos.*") and other internal services such as "urn:nena:service:agencyLocator". If the data in the internal and external ECRFs are different, this would only affect service boundary data. All LVFs are provisioned with the same data, whether inside or outside the ESInet.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 44	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Accessibility Inside the ESInet** Contractor shall provide an ECRF accessible inside an ESInet, which shall permit querying from any PSAP (or future entity authorized to connect to the ESInet) inside the ESInet. ECRFs provided by other entities may have their own policies regarding who may query them. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: NGA 911 will implement our comprehensive and fully NENA i3 standardized ECRF solution as an integral part of our NGCS offering to the state of Nebraska. NGA 911's ECRF will be configured to accept LoST queries from any entities that the State of Nebraska authorizes. As specified in the NENA-STA-10.2-2016 the Emergency Services IP network (ESInet) must support ECRF's both "external" and "internal" to the ESInet as applicable. The NGA 911 ECRF permits querying from both internal and external ECRF's. ECRF's provided by other entities whether internal or external may have their own policies about who may query them. If such ECRF's are hosted externally, NGA 911 will interface with them through a secure bilateral Border Control Function (BCF) interface or equivalent. An external ECRF normally need only have the external (which ESInet) route for "urn:service:sos.*" The internal ECRF also needs routes for ESRP use ("urn:nena:service:sos.*") and other internal services such as "urn:nena:service:agencyLocator". NGA 911 will coordinate with ECRF owners whether an OSP, ESInet, State Agency, or PSAP and its GIS vendor to ensure that the NGCS ECRF is properly validated against the authoritative ECRF so that all routing changes in the State of Nebraska's ECRF/LVF for call routing and route verification. The ESRP will query the NGCS ECRF for routing as a default but can also access the State's. In any case the NGCS ECRF will be a mirror of the State's and the NGCS LVF will be validated against the authoritative LVF.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 45	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Origination Network ECRF** An origination network may use an ECRF, or a similar function within its own network, to determine an appropriate route—equivalent to what would be determined by the authoritative ECRF—to the correct ESInet for the emergency call. Describe the functionality of such an ECRF equivalent and document where this functional element resides within the proposed solution.	X			
	Bidder Response: An origination network may use an ECRF, or a similar function within its own network, to determine an appropriate route, to which the State of Nebraska ECRF is authoritative. The NGCS ECRF supports a routing query interface that can be used by an endpoint, ESRP, or PSAP to request location-based routing information from the ECRF. Additionally, it supports both iterative and recursive queries to external ECRF sources. The ECRF interfaces with the Location to Service Translation (LoST) protocol (RFC5222) and supports LoST queries via the ESRP, PSAP customer premise equipment (CPE), or any other permitted IP host. The proposed ECRF also allows for rate limiting queries from sources other than the proposed ESRP(s), and provides logging of all connections, connection attempts, and LoST transactions.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 46	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Routing Query Interface** The ECRF shall support a routing query interface that can be used by an endpoint, ESRP or PSAP to request location-based routing information from the ECRF. Additionally, it shall support both iterative and recursive queries to external ECRF sources. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The NGA 911 ECRF is standardized on Location-to-Service Translation (LoST) as the main routing query interface to ESRPs and PSAPs. Although the NGA 911 does support both iterative and recursive queries, by default NGA 911 recommends configuring the ESInet to utilize the recursion as the default query mode to ensure the fastest response.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 47	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **LoST Protocol Support** The ECRF shall interface with the Location-to-Service Translation (LoST) protocol (as described in IETF RFC 5222) and support LoST queries via the ESRP, PSAP CHE, or any other permitted IP host. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: NGA 911 utilizes the Location to Service Translation (LoST) protocol as described in IETF RFC 5222 to support Lost queries via the ESRP, PSAP CPE or any other permitted IP host.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 48	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Query Rate-Limiting** The proposed ECRF shall allow for rate-limiting queries from sources other than the proposed ESRP(s), and provide logging of all connections, connection attempts, and LoST transactions. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: The NGA 911 solution will support rate-limiting queries. Queries from sources other than the ESInet ESRP may also come through the BCF/SBC and any rate-limiting will also be applied at that point. Otherwise, the ECRF provides logging of all connections, connection attempts, and LoST transactions.				

Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS) **Emergency Call Routing Function (ECRF)** **Supported Functions** The ECRF shall support each of the following items. Describe how the solution meets or exceeds each of the requirements below:	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 49	Bidder Response: The NGA 911 ECRF is fully compliant with NENA Detailed Functional and Interface Standards for the NENA i3 Solution NENA-STA-010 and NENA -2-014 and provides routing information (location based) and location validation information to the network for State of Nebraska. The proposed solution: **Logging of all connections, connection attempts, data updates, ECRF query results and LoST transactions** The ECRF provides logging of all connections, connection attempts, successful data uploads, errors in data uploads, ECRF query results, and LoST transactions. NGA 911 provides for error handling, default routing, and logging. The ECRF handles LoST error conditions per RFC 5222 and provides at least a default route set up by the administrators on a geographic basis. The system provides extensive logging that can be used as necessary by NG9-1-1 loggers. **Location error correction** Errors are prevented from being uploaded into the ECRF/LVF. Our SI provides QA/QC that safeguards errors to be loaded, this is to protect mis-routes due to faulty data. NG9-1-1 calls will only be routed on QA/QC routable data. We will work with the Commonwealth to perform QA/QC once we receive the GIS data. The SI is designed to QA/QC errors with	X			

	your jurisdiction and your neighboring jurisdictions in order to avert call routing errors entering the ECRF. **Updates from the SI in near real-time with no degradation of LoST services** The NGA 911 SI provides GIS data updates to the ECRF and LVF. Authorized 9-1-1 authorities can utilize SI services provided by NGA 911 via our Web-Portal. This reduces the load on the ECRF to maintain efficiency in request/response activities. Valid data flows from the LVF to the ECRF with no disruption or degradation to LoST query responses. This flow can be configured to be as quick as "near real time" to a specific time interval to allow for any approval cycles. **Routing of calls based on geographic coordinates, geodetic shapes and civic addresses** Our solution routes calls using Lat/Long, civic address information, geodetic shapes. The ECRF queries access geocoding functionality and PSAP location data and produce validated Uniform Resource Identifier (URI) routes. **Utilization of common GIS boundaries, including, but not limited to, PSAP, law enforcement, fire and emergency medical services (EMS)** Our solution can use all common GIS boundaries that include but not limited to, PSAP, law enforcement, fire and emergency medical services (EMS). Our solution utilizes all of the NENA Reuired and Strongly Recommended layers and will work with your local GIS. We formulate the proper response based on the findService URN provided in the LoST query. We support all of the query types defined in RFC 5222 with all common inputs (e.g., civic, x/y, etc.)				

	Permitting of LoST queries for find-service-request association with each layer Depending on the sophistication of the neighboring ECRF, we could use LoST Synch (RFC 6739), Web Feature Service (WFS), or some form of batch data exchange to permit LoST queries for find-service-request association with each layer. If an FG exists, we would propagate the ECRF coverage area data to the next level higher in the hierarchy as per NENA's specifications. **Compliance with NENA 02-010 and NENA 02-014** The NGA 911 ECRF is fully compliant with NENA Detailed Functional and Interface Standards for the NENA i3 Solution NENA-STA-010 and NENA -2-014 and provides routing information (location based) and location validation information to the network for the State of Nebraska. **Dynamic updates to GIS without disruption of the ECRF** Each ECRF element maintains two copies of each map layer, an active one that processes the LoST queries and an inactive one. New updates are applied to the inactive directory. Once processing is complete for all ECRF computing elements, the ECRF system will notify the SI that the load was successful and make the inactive map layer active. If for some reason the load was unsuccessful, the ECRF system will pass that result along to the SI which will send out alarm notifications to authorized members. If this occurs the previously active map layer will remain active. It is recommended that new updates not be sent until the notification has been received from the SI that the previous update has finished processing. **Validation of GIS updates before they are provisioned into the ECRF**				

	GIS updates are provisioned through the SI which performs GIS validations, including validations to ensure routing integrity. The Quality Assurance and Quality Control (QA/QC) processes/validation provided during validation steps in the SI prior to provisioning the ECRF to prevent any unwanted gaps or overlaps from being provisioned in the ECRF. All validation and alarming functions associated with the NGA 911 ECRF are handled on servers independent of those supporting the call-time ECRF functions to ensure that these "provisioning" functions do not interfere with the critical call path functions of the ECRF.				

Any additional documentation can be inserted here:

	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
Logging of all connections, connection attempts, data updates, ECRF query results, and LoST transactions	X			
Location error identification.	X			
Updates from the SI in near real-time with no degradation of LoST services	X			
Routing of calls based on geographic coordinates, geodetic shapes, and civic addresses	X			
Utilization of common GIS boundaries, including, but not limited to, PSAP, law enforcement, fire and emergency medical services (EMS).	X			
Permitting of LoST queries for find service request association with each layer.	X			
Compliance with NENA 02-010 and NENA 02-014.	X			
Dynamic updates to GIS without disruption of the ECRF.	X			
Validation of GIS updates before they are provisioned into the ECRF.	X			

	Next Generation Core Services Elements (NGCS) **Emergency Call Routing Function (ECRF)** **User Interface and Provisioning** Define bidder's method for: 1. provisioning the ECRF; 2. updating the ECRF (including the frequency of updates); 3. validating data provisioning; 4. performing error logging; 5. performing gap and overlap analysis; and 6. supporting LoST queries from ESRPs, the PSAP CHE, and other authorized hosts within the ESInet. 7. Provide a clear description of the functionality of the ECRF; list features and capabilities; 8. describe the error handling, default mechanisms, and logging; and 9. provide an overview of deployment recommendations to achieve 99.999 percent reliability.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
NGCS 50	Bidder Response: Bidder Response: 1. The ECRF will be provisioned exclusively from the statewide GIS system. This single GIS repository will be the authoritative source of all GIS data. 2. All updates will come from the GIS repository directly; they will occur once every 24 hours at a regularly scheduled time that normally has relatively low traffic flow. An update can be flagged as urgent that will push out an update to the ECRF immediately. 3. The Quality Assurance and Quality Control (QA/QC) processes provided during the validation steps in the SI will prevent any unwanted gaps or overlaps from being provisioned in the ECRF. A change control system will be available to monitor and manage data discrepancies and to track data change requirements. 4. Errors from the validation process will be logged in a tabular form and output by our automated QA/QC process into a DR. 5. The Quality Assurance and Quality Control (QA/QC) processes provided during the validation steps in the SI will prevent any unwanted gaps or overlaps from being provisioned in the ECRF. 6. The ECRF supports LoST querying from all authorized elements in the ESInet. This support extends to all PSAPs, subordinated ECRFs, and CHEs. 7. The ECRF will process 9-1-1 calls and sessions routed with the appropriate (URI) from the ESRP. The ESRP enables the acquisition of a PSAP-routable address by invoking the ECRF. The ECRF will acquire the location by one of two methods.				

	Either by reading a valid address directly embedded inside the call itself or by querying an external data source based on an embedded reference in the call. 8. To handle records that result in errors or warnings, a governance body review of DRs would be expected on an average weekly basis with the management and technical leads for the respective aspects of the LVF. Our management approaches will accommodate the conditions where critical discrepancies require emergency responses. Our GIS Tools will allow for approved Manual editing as required as well with a set of approved scripts and approval gates which will then use the aforementioned data pipeline process to perform the acquisition, ingestion, validation & augmentation and ledger recording. The resolution of the discrepancy will be coordinated with the reporting agency and ESInet operational management, and/or appropriate Governance body to align with established change management procedures for data and other configuration items. 9. NGA 911 recommends the implementation of a single ECRF for the entire state of Nebraska. This solution will be hosted in the cloud that will always be running 8 redundant instances of the ECRF simultaneously in widely distributed geographical areas of the United States. Any of these 8 instances can immediately take over the load from any of the others ensuring reliability that exceeds five 9s. The geographic distribution with independent facilities reduces the chances of a service outage entirely to almost zero.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 51	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Hierarchical Integration with Other ECRFs** The ESInet will be part of an overall hierarchical plan that includes interconnectivity to other regions and ECRFs. Provide details regarding bidder's vision for how this interconnection will include replicas of ECRF/LVF at different levels of the hierarchy, as well as access/origination networks.	X			
	Bidder Response: Given the current status of a national Forest Guide (FG), we are designing our approach to the ECRF interconnectivity on a basis of cooperation rather than the end-state use of an FG. NGA 911 will work with neighboring ECRF providers to agree upon a regular exchange of coverage area information. We will agree on a mechanism and periodicity. Depending on the sophistication of the neighboring ECRF, we could use LoST Synch (RFC 6739), Web Feature Service (WFS), or some form of batch data exchange. If an FG exists, we would propagate the ECRF coverage area data to the next level higher in the hierarchy as per NENA's specifications. The NGA 911 NG9-1-1 Core Services (NGCS), in compliance with this RFP and as a key component of any NGCS, provides a completely functional ECRF/LVF that can operate as the Prime ECRF for the routing. As specified in the NENA-STA-10.2-2016 the Emergency Services IP network (ESInet) must support ECRF both "external" and "internal" to the ESInet as applicable. For Nebraska this will include the other ECRF/LVF which can be hosted either externally or internally to the ESInet. If it is hosted externally, NGA 911 will interface with the State's ECRF/LVF through a secure bilateral Border Control Function (BCF) interface or equivalent. An external ECRF normally need only have the external (which ESInet) route for "urn:service:sos.*" The internal ECRF also needs routes for ESRP use ("urn:nena:service:sos.*") and other internal services such as "urn:nena:service:agencyLocator". However, we envision a solution where the authoritative ECRF is mirrored by the internal ECRF that provides routes for the ESRP. All LVFs are provisioned with the same data, whether inside or outside the ESInet. NGA 911 will coordinate with ECRF owners whether an OSP, ESInet, State Agency, or PSAP and their GIS vendors to ensure that the NGCS ECRF is properly validated against the authoritative ECRF so that all routing changes in the respective ECRF/LVF for call routing and route verification. The ESRP will query the NGCS ECRF for routing as a default. In any case the NGCS ECRF will be a mirror of the State of Nebraska's and the NGCS LVF will be validated against the authoritative LVF.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 52	**Next Generation Core Services Elements (NGCS)** **Emergency Call Routing Function (ECRF)** **Forest Guide** Provide explanations of any tradeoffs between aggregations of data at higher-level ECRFs versus the use of Forest Guides (as defined in NENA-INF-009.1-2014) to refer requests between ECRFs that possess different levels of data. As part of that explanation, provide details on how the appropriate ECRF/LVF data will be managed and provisioned for use in overload and backup routing scenarios in the current environment, and any dependencies that might impact provisioning.	X			
	Bidder Response: NGA 911's solution is flexible enough to aggregate data progressively and hierarchically or make use of a Forest Guide. Although NGA 911 provides the ability to use these techniques we think a single authoritative ECRF for the entire state ESInet is operationally the simplest and coincidentally the most efficient approach to implementing the ECRF functionality. The Nebraska ESInet will then become a single "tree" in the National Forest Guide when it is finally ready. The initial provisioning of the ECRF will be done through an SI setup to interface with the state's GIS database. The Quality Assurance and Quality Control (QA/QC) processes provided during the validation steps in the SI will prevent any unwanted gaps or overlaps from being provisioned in the ECRF. A change control system will be available to monitor and manage data discrepancies and to track data change requirements. Validated GIS updates are normalized and applied to the ECRF production instances in a manner that preserves availability and coordinates with other ESInet scheduled updates and activities. Updating the ECRF with the latest information published in the statewide GIS will be scheduled to occur automatically once a day at a set time chosen by NGA 911 and the state. If there is a requirement for an immediate update the GIS will be able to push it out to the ECRF in the cloud where each of the 8 redundant instances of the ECRF will be updated serially. After the first one is updated our system will automatically start using the updated instance to serve all queries initially, as other instances of the ECRF are updated the LoST queries will be evenly distributed among them. The ECRF that NGA 911 is proposing will be hosted in our partner's (Amazon Web Services) cloud. NGA will be running 8 concurrently, fully redundant and geographically widespread instances of the ECRF. Each of those instances can automatically and dynamically (and practically instantaneously) scale the amount of processing, storage and memory required to meet whatever demand is required or expected. This dynamic capability and redundancy allow our solution to handle whatever backup or overload scenarios that might occur in the state.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 53	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** An LVF is a LoST protocol server where civic location information for every call originating endpoint is validated against the SI-provisioned GIS data Describe how the LVF solution interfaces with other LVF solutions which may interface with bidder's solution. Contractor shall coordinate with other LVF solution providers to ensure interoperability between the respective solutions.	X			

Bidder Response:

The NGA 911 LVF is the authoritative LVF for the deployment and is validated against the SI-provisioned GIS. GIS updates are provisioned through the SI which performs GIS validations, including validations to ensure routing integrity. The Quality Assurance and Quality Control (QA/QC) processes provided during validation steps in the SI will prevent any unwanted gaps or overlaps from being provisioned in the LVF. A change control system is established to monitor and manage data discrepancies and to track data change requirements. Validated GIS updates are normalized and applied to the LVF production instances in a manner that preserves availability and coordinates with other ESInet scheduled updates and activities.

To handle records that result in errors or warnings, a governance body review of DRs would be expected on an average weekly basis with the management and technical leads for the respective aspects of the LVF. Our management approaches will accommodate the conditions where critical discrepancies require emergency responses. Our GIS Tools will allow for approved Manual editing as required as well with a set of approved scripts and approval gates which will then use the aforementioned data pipeline process to perform the acquisition, ingestion, validation & augmentation and ledger recording.

Then as the authoritative LVF, the LVF interfaces to other LVFs through a similar QA/QC process as defined above with the GIS SI.

Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS) **Location Validation Function (LVF)** **LVF Description** . The SI is responsible for provisioning and updating the information used for location validation in the LVF, which shall contain a standardized interface to the SI. Describe how the LVF solution meets the above requirements**.**	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 54		X			

Bidder Response:

The key success factor to working with the statewide GIS is the alignment of the NGA 911 SI with the GIS database formats, processes, flows, validation and discrepancy reporting (DR) methods. Our SI essentially converts the data layers in the GIS database to make them easily and automatically consumable by the NGA 911 ECRF/LVF and our LDB/LIS

GIS SI validation of ECRF and LVF: The provision of GIS updates will occur through the SI which performs GIS validations, including validations to ensure routing integrity. The Quality Assurance and Quality Control (QA/QC) processes provided during the validation steps in the SI will prevent any unwanted gaps or overlaps from being provisioned in the ECRF. A change control system will be available to monitor and manage data discrepancies and to track data change requirements. Validated GIS updates are normalized and applied to the ECRF production instances in a manner that preserves availability and coordinates with other ESInet scheduled updates and activities.

Initial SI Integration: NGA 911 intends to proactively employ an Agile approach using a collaborative discover, define, design approach working with Nebraska, to help ensure a smooth integration of our SI with the GIS DB rather than the standard way to do this which often is to be reactively or passively auditing the DB at delivery receipt later pointing out the flaws. Led by our Professional Certified GIS Analysts (GIS-P) with deep experience in federal and state address, point features, and boundaries, NGA 911 will assess the following to establish the business rules and configuration.

Operation and Maintenance of SI: After the initial setup and verification of the SI and the interfaces and process flows between LVFand the GIS Repository; NGA 911 provides the following tools, processes, and methodologies for operating and maintaining the SI:

Step 1: Data Acquisition: We have built in a collaborative approach to discover, define, and design to a model where we will reflect in our LVF of all changes from statewide GIS. Changes will only be received via the Statewide GIS through the scheduled or notification API Call via SI based on agreed NENA compliant version management filters to determine the updates, inserts, and deletes to

	request. Configured sources will have drop folders automatically created by pre-configured feed parameters. To support proper file loading, compliance will support NENA-STA-005.1.1-2017 Provisioning and Maintenance of GIS data to ECRFs and LVFs, NENA-STA-010.2 NENA Detailed Functional and Interface Standards for the NENA i3 Solution, and NENA STA-015.10-2018 (Originally 02-010) Data Formats for E9 1 1 Data Exchange & GIS Mapping. **Step 2: Data Ingestion:** Once the file or service request is received, the received records will queue to support data ingestion into the ECRF, LVF, and LDB. To support near real-time queuing of record processing at over 1,000 records/minute, step 1 loaded files will trigger scripts to then decompose such files into individual GeoJSON records (files) by every Feature ID. This is a 'technical background step' with the highest scalability and most robust data processing environment. This ends up populating the Step 3 Queue with each record, ready for processing in accordance with NENA 02-014 v1 GIS Data Collections and Maintenance Standards and REQ 002 NG9-1-1 Data Management Requirements guidance. The system will accommodate ad-hoc changes, expedited changes, and a standard planned update process to ensure the most recent and vital information is available to assist callers and first responders. Updates occur on at least a daily basis, unless the update has an effective "on date." The ECRF data administration tool uses a role-based workflow with the capacity to support staging updates, and coordinates, at a minimum, receiving data updates 24x7x365 and providing a confirmation of receipt of data within 24 hours. **Step 3: Data Validation & Augmentation:** Each record will process by the associated feature class modular QC scripts written per NENA Standards/requirements based on Transition Business Rules Design to accommodate the third-party GIS data model, rules, attributes, etc. This will allow us to take the other parties standards and our standards to make it work with the statewide GIS database. Records in the SI Patch or files receiving change request are in drop sub-folders which associate the proper feature class and source authority business rules script. Validation Scripts can support rules and comply with NENA 71-501 Geospatial Attribute Data Validation and Topologic Data Validation, field mapping to NG9-1-1 GIS Data Model NENA-STA-006.1-2018, geocoding augmentation, and support DR handling per Section 3.4.4 DR of NENA INF 014.1-201 and 20150120_ISF NG9-1-1 GIS Data Compilation and Stewardship Charter 20151209. Each processed record will have state recorded (e.g., accepted, warning, failure) for the next step. Once processing is complete for all ECRF computing elements, the ECRF/LVF system will notify the SI that the load was successful and make the inactive map layer active. If for some reason the load was unsuccessful, the ECRF/LVF system will pass that result along to the SI which will send out alarm notifications. If this occurs, the previously active map layer will remain active. It is

	recommended that new updates not be sent until the notification has been received from the SI that the previous update has finished processing. **Step 4: Publishing and Ledger Merging:** Based on Transition Business Rules Design, the ledger will handle the warnings and failures per cited Governance standards, and accepted records will be identified as new, changed, same, or to be removed.

Any additional documentation can be inserted here:

NGCS 55	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** **Location Validation** The LVF shall be available to validate civic locations at the time a wireline device is ordered— e.g., Service Order Interface (SOI) validation—when a nomadic device is connected to the network, and when a PSAP or other authorized entity makes a civic location validation request. The LIS/LDB shall be allowed to periodically revalidate the civic location information against the GIS data contained within the LVF. Describe how the solution meets or exceeds the above requirements.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: The NGA 911 LVF solution is available to validate civic locations at the time a wireline device is ordered, i.e., service order interface (SOI validation, when a nomadic device is connected to the network and when a PSAP or other authorized entity makes a civic location validation request. The LIS/LDB will periodically revalidate the civic location information against the GIS data contained within the LVF.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 56	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** **High-Availability Design** The LVF shall support all functionality as defined in NENA-STA-010.2-2016, shall be designed with resiliency and redundancy to provide a minimum of 99.999 percent availability, and shall be provisioned with the same data as the ECRF. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: In NGA 911's implementation the LVF and ECRF are a combined single entity with two functional elements so automatically share the same data. This ensures that there is no gap between the two datasets. Our approach removes any potential errors and signaling overhead that can result from synchronizing two different databases. NGA 911's NGCS (including the LVF) is 100% deployed in the cloud, providing the best possible reliability and availability in the industry. All functional elements (FE) of the NGA 911 NGCS are designed, architected, and deployed on the AWS Cloud in a manner which strictly adheres to the criteria defined in NENA-STA-010.2-2016 for an NGCS. All Amazon Web Services (AWS) data centers and direct connect facilities are designed to an Uptime Institute level of Tier III+ or above. The NGA 911 solution is fully redundant, deploys dual Cores in four (4) Availability Zones (AZ) for a total of eight (8) LVFs. The AWS AZs are required to be a minimum of 10 miles apart and on separate power grids. The AZs are connected by multiple high-speed broadband carriers in meshed networks. Having 8 cores allows NGA 911 to exceed Nebraska's five 9s availability requirement.				

NGCS	*Non Redundant 1 AZ*		*Redundant 2 AZ*		*Redundant Region 2 AZ's each*	
Functional Element	**Signaling**	**Media**	**Signaling**	**Media**	**Signaling**	**Media**
AWS Data Element	*99.999%*	*99.999%*	*>99.999%*	*>99.999%*	*100%*	*100%*
BCF	*99.99%*		*>99.999%*		*100%*	
ESRP	*99.95%*	*99.95%*	*>99.999%*	*>99.999%*	*100%*	*100%*
ECRF	*99.95%*		*>99.999%*		*100%*	
LVF	*99.95%*		*>99.999%*		*100%*	
	99.84%	**99.95%**	**>99.999%**	**>99.999%**	**100%**	**100%**

**100% signifies many 9's above five 9's*

Each of the 8 LVFs are architected to support 100% of the traffic for Nebraska. The NGA 911 cores operate in an active-active mode. SIP Signaling is processed through the eight (8) cores dedicated to Nebraska utilizing a load balancing round robin approach that ensures all network FE's are constantly and consistently exercised. In the event of failure of any one stack, that supporting core infrastructure is taken offline and replaced with a new container of the instance without effect to the other operational cores. This approach ensures that there is never a gap in availability and exceeds the five 9s requirements defined by Nebraska. 100% of the platform capacity will survive any single element of the solution experiencing a failure.

Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS) **Location Validation Function (LVF)** **Public-Facing LVF** Outline options for a public-facing LVF provisioned for use by service providers outside the ESInet.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
NGCS 57	Bidder Response: NGA 911 proposes implementing a single ECRF/LVF for the entire state of Nebraska. The LVF capability will not only be accessible internally inside the ESInet but also externally by the OSPs for the validation of their civic addresses that will ultimately be loaded into the statewide LIS. Queries to the LVF will all be performed through the LoST protocol over the BGP transport layer. The LVF shall be made available via an LVF proxy in the public internet in a secure, controlled manner provided by NGA 911 for OSPs and other Nebraska authorized entities. NGA 911 will deploy the LVF instance(s) separate from the ECRF instances to ensure that bulk validations do not affect call routing. It is noted that very few (if any) originating service providers currently operate a LIS that would take advantage of a public facing validation source.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 58	**Next Generation Core Services Elements (NGCS)** **Location Validation Function (LVF)** **User Interface and Security** Describe the functionality of the proposed LVF solution in sufficient detail to address the requirements outlined in NENA-STA-010.2-2016, with particular attention to: 1. the arrangement of the proposed components; 2. user interface and features; 3. and security aspects.	X			

Bidder Response:

1. The NGA 911 solution is a fully functional ECRF/LVF that complies with all NENA and IETF standards and provides full migration into i3 without costly technology acquisition and process overhaul. Key aspects of the solution include:

    - Allows data analysts to correlate street and community names from three data sources (Postal, MSAG, and GIS) prior to call routing, providing three layers of routing data support. This is unique in the industry and provides the most effective way to prevent default call routing.
    - Allows authorized service providers to validate locations prior to call routing using real time data.
    - Integration with 9-1-1 DBMS: MSAG, ALI, LIS, LDB,SI.
    - Identifies common error discrepancies between MSAG, GIS, and Postal.
    - Extensive online help.
    - Extensive security mechanisms allow access and updating tailored to most organizations' data operations.
    - Links to online mapping resources.
    - Web-based user interface for ease of data management.
    - Extensive reporting capabilities including 17 reports – all of which can be exported to Excel, PDF, etc. A tracking agency and individual progress in data preparation.
    - Allows establishment of translations including County (e.g., "007" = "Boone County"), Community (e.g., "North Boone" = "Beaverton") and Street (e.g., "SH 76" = "Fairground Rd." = "State Line Rd.").

2. The NGA 911 LVF solution has an intuitive web-based user interface. This allows analysts to manage aliases, determine search hierarchies, view discrepancies, etc. It also has an easy to use interface that allows the analyst to enter a location (either civic or geodetic) and it will format the proper LoST request and submit it to the server. This allows testing of reported discrepancies without having to interact with the XML that is behind the scenes.
3. The LVF is secured through a combination of authorized use certificates, VPN, and direct connections. All traffic is subject to IPSec tunneling, and subscribers are not able to modify the data when performing a LoST query. The QA/QC process is conducted separately using the secure SI.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 59	**Next Generation Core Services Elements (NGCS)** **Spatial Interface (SI)** **SI Description** The SI is responsible for provisioning and updating authoritative GIS data to the ECRF, the LVF, the map viewer, the PSAP tactical map display, CAD systems, and similar applications that consume GIS data. GIS data provisioned by the SI shall undergo data-quality and data-integrity checks to ensure that the data complies with all applicable requirements of NENA 02-010, NENA 02-014, and Attachment B of NENA-STA-010.2-2016. Describe how the solution meets or exceeds the above requirements.	X			

Bidder Response:

The key success factor to working with the statewide GIS is the alignment of the NGA 911 SI with the GIS database formats, processes, flows, validation and discrepancy reporting (DR) methods. Our SI essentially converts the data layers in the GIS database to make them easily and automatically consumable by the NGA 911 ECRF/LVF and our LDB/LIS

GIS SI validation of ECRF and LVF: The provision of GIS updates will occur through the SI which performs GIS validations, including validations to ensure routing integrity. The Quality Assurance and Quality Control (QA/QC) processes provided during the validation steps in the SI will prevent any unwanted gaps or overlaps from being provisioned in the ECRF. A change control system will be available to monitor and manage data discrepancies and to track data change requirements. Validated GIS updates are normalized and applied to the ECRF production instances in a manner that preserves availability and coordinates with other ESInet scheduled updates and activities.

Initial SI Integration: NGA 911 intends to proactively employ an Agile approach using a collaborative discover, define, design approach working with Nebraska, to help ensure a smooth integration of our SI with the GIS DB rather than the standard way to do this which often is to be reactively or passively auditing the DB at delivery receipt later pointing out the flaws. Led by our Professional Certified GIS Analysts (GIS-P) with deep experience in federal and state address, point features, and boundaries, NGA 911 will assess the following to establish the business rules and configuration.

Operation and Maintenance of SI: After the initial setup and verification of the SI and the interfaces and process flows between the ECRF/LVF and the GIS Repository; NGA 911 provides the following tools, processes, and methodologies for operating and maintaining the SI:

	Step 1: Data Acquisition: We have built in a collaborative approach to discover, define, and design to a model where we will reflect in our LVF of all changes from statewide GIS. Changes will only be received via the Statewide GIS through the scheduled or notification API Call via SI based on agreed NENA compliant version management filters to determine the updates, inserts, and deletes to request. Configured sources will have drop folders automatically created by pre-configured feed parameters. To support proper file loading, compliance will support NENA-STA-005.1.1-2017 Provisioning and Maintenance of GIS data to ECRFs and LVFs, NENA-STA-010.2 NENA Detailed Functional and Interface Standards for the NENA i3 Solution, and NENA STA-015.10-2018 (Originally 02-010) Data Formats for E9 1 1 Data Exchange & GIS Mapping. **Step 2: Data Ingestion:** Once the file or service request is received, the received records will queue to support data ingestion into the ECRF, LVF, and LDB. To support near real-time queuing of record processing at over 1,000 records/minute, step 1 loaded files will trigger scripts to then decompose such files into individual GeoJSON records (files) by every Feature ID. This is a 'technical background step' with the highest scalability and most robust data processing environment. This ends up populating the Step 3 Queue with each record, ready for processing in accordance with NENA 02-014 v1 GIS Data Collections and Maintenance Standards and REQ 002 NG9-1-1 Data Management Requirements guidance. The system will accommodate ad-hoc changes, expedited changes, and a standard planned update process to ensure the most recent and vital information is available to assist callers and first responders. Updates occur on at least a daily basis, unless the update has an effective "on date." The ECRF data administration tool uses a role-based workflow with the capacity to support staging updates, and coordinates, at a minimum, receiving data updates 24x7x365 and providing a confirmation of receipt of data within 24 hours. **Step 3: Data Validation & Augmentation:** Each record will process by the associated feature class modular QC scripts written per NENA Standards/requirements based on Transition Business Rules Design to accommodate the third-party GIS data model, rules, attributes, etc. This will allow us to take the other parties standards and our standards to make it work with the statewide GIS database. Records in the SI Patch or files receiving change request are in drop sub-folders which associate the proper feature class and source authority business rules script. Validation Scripts can support rules and comply with NENA 71-501 Geospatial Attribute Data Validation and Topologic Data Validation, field mapping to NG9-1-1 GIS Data Model NENA-STA-006.1-2018, geocoding augmentation, and support DR handling per Section 3.4.4 DR of NENA INF 014.1-201 and 20150120_ISF NG9-1-1 GIS Data Compilation and Stewardship Charter 20151209. Each processed record will have state recorded (e.g., accepted, warning, failure) for the next step.

	Once processing is complete for all ECRF computing elements, the ECRF/LVF system will notify the SI that the load was successful and make the inactive map layer active. If for some reason the load was unsuccessful, the ECRF/LVF system will pass that result along to the SI which will send out alarm notifications. If this occurs, the previously active map layer will remain active. It is recommended that new updates not be sent until the notification has been received from the SI that the previous update has finished processing. **Step 4: Publishing and Ledger Merging:** Based on Transition Business Rules Design, the ledger will handle the warnings and failures per cited Governance standards, and accepted records will be identified as new, changed, same, or to be removed.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 60	**Next Generation Core Services Elements (NGCS)** **Spatial Interface (SI)** **Web Feature Service and Updates** The SI shall convert the GIS data into the format (data structure and projection) used by the ECRF and LVF, in real-time or near real-time, using a web feature service. The SI shall be able to provision and perform incremental updates, in near real-time, to the ECRF, LVF, the map viewer service, the PSAP tactical map display and similar applications that consume GIS data. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: NGA 911 has implemented and is implementing SIs for various public safety jurisdictions and has a default code base that works efficiently and can load GIS data to all "subscribers" with near real-time efficiency. The SI though needs to be customized for each GIS implementation as they are all unique. NGA 911 intends to proactively employ an Agile approach using a collaborative discover, define, design approach working with Nebraska, to help ensure a smooth integration of our SI with the GIS DB rather than the standard way to do this which often is to be reactively or passively auditing the DB at delivery receipt later pointing out the flaws. Led by our Professional Certified GIS Analysts (GIS-P) with deep experience in federal and state address, point features, and boundaries, NGA 911 will assess the following to establish the business rules and configuration. NGA 911 solution will provide a web interface and/or automated method to provision 9-1-1 to the SI and retrieve post-QA data for the use of maps and/or the computer-aided dispatch (CAD) system.				

Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS) **Spatial Interface (SI)** **Data Provisioning and Validation** Describe the functionality of the proposed SI solution in sufficient detail to explain the validation of GIS data and data updates prior to provisioning into the ECRF and LVF, along with the means of real-time or near real-time provisioning of incremental updates to the GIS data provisioned to the ECRF and LVF.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 61		X			

Bidder Response:

The NGA 911 solution is able to provision and update authoritative GIS data provided by the SI to the ECRF, the LVF, and provision data quality and data integrity (QA/QC) checks to ensure the data complies with all applicable requirements of NENA 02-010, NENA 02-014, and Attachment B of NENA-STA-010.2-2016.

The need for accurate GIS data does not stop at the county line. Recognizing this, NGA 911 built master GIS repository application to fulfill the role of NENA's i3 SI Function (SIF). As each PSAP provisions a copy of their GIS data, it will perform validation checks as SpatialStation does (as described above) but will also consider adjacent jurisdictions for future validation needs.

Key product features include:

- 24x7 real-time GIS data upload access
- Automated reprojection of data to WGS-84
- On-the-fly topological and attribution validation checks
- Gap / Overlap detection
- GIS database support for 'Shape File' and 'File Geodatabase' Esri formats
- Dynamic field mapping to accommodate local GIS database structures
- Road Centerline, Address Point and Polygon feature class analysis
- Live and fully interactive map display of validation errors location and type
- Dashboard monitoring for data uploads, downloads, user notification and error counts
- Automated email notifications for users and system administrators
- Activity history tracking and reporting
- Secure User Login for users and system administrators
- Fully Esri compliant application

Nga 911 will automatically send valid GIS data to both LVF and ECRF. When the State of Nebraska is ready, this data can be delivered to any other endpoint either through Web Feature Service (WFS) or file exchange (e.g., SHP file or file geo-database).

	Nga 911 has integrated PSAP tactical map display, CAD systems and similar applications that utilize GIS data. This can also be any other end point that can accept a WGS feed or a file geo-database. The NGA 911 solution has the ability to be automated and manual in the GIS upload process. When a version of the GIS data is uploaded the systems validate and log the load was successful or unsuccessful. The log is in a closed loop configuration.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 62	**Next Generation Core Services Elements (NGCS)** **Spatial Interface (SI)** **Use of the Commission's GIS Data Model** 1. Describe how the bidder's solution will use the Commission's GIS data model (Attachment B) without modification to the schema. 2. Define bidder's processes and methods to receive and incorporate the updated SI datasets. 3. Describe bidder's proposed workflow for receiving GIS updates from regions to allow for a smooth transition. 4. Describe all security and monitoring aspects, and any additional features supported by the proposed SI.	X			
	Bidder Response: According to the description in Attachment B the Commissions data is properly aligned with the relevant NENA GIS standards and should have no problem being ingested into the GIS as is and then further incorporated into the ECRF/LVF and LDB through the SI that will be developed. Our default GIS information update schedule for our SI "subscribers" is once a day (this can easily be altered if Nebraska wants a faster or slower pace). If a change to the GIS is defined as critical the SI will push out an update immediately to the "subscribers". If there are multiple ECRFs (ESInet internal or external) they will all receive their update from the authoritative ECRF rather than from the SI. The NGA 911 NGCS will receive its updates from a single source-of-truth statewide GIS. GIS updates from the regions should flow up to the statewide NENA compliant GIS to be managed and QA/QCed centrally. From that single central GIS all updates are made to the NGCS functional elements through the SI. The NGCS in that way is not receiving GIS updates directly from the regions but through the SI that is configured to interface with the statewide GIS repository. NGA 911's SI conforms to all the relevant security and monitoring NENA standards and will only be accessible by entities authorized to use the SI. From a security and multi-jurisdictional perspective, the ecosystem described above also: • Allows replication intervals to be set to allow time for review and approval. • Requires unique log on credentials to each system. • Each user is assigned a role and is identified by an authoritative boundary polygon that dictates where they are allowed to affect data. • Web based systems are secured with SSL encryption.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 63	**Next Generation Core Services Elements (NGCS)** **Location Database (LDB)** Describe how the solution interfaces with other LDB solutions which may participate in or interface with bidder's solution. Contractor shall coordinate with other LDB solution providers to ensure interoperability between the respective solutions. Also explain how the proposed solution would deal with multiple ALI/MSAG databases and the locations where ALI steering may be in place.	X			
	Bidder Response: NGA 911 takes the approach that a single LDB should be deployed to cover the whole state of Nebraska as it transitions to a full blown NG9-1-1 installation and adopts the LIS. If there are multiple regional ALI databases currently operational in the state, NGA will work with each of the regions to migrate their databases over to the unified statewide LDB. That will hold the whole state's MSAG/ALI tabular data. Authorized external entities such as OSPs will be given access to the LDB to validate and upload ALI/MSAG information. PSAPs that have not been fully cutover to the NGCS will still be able to query the LDB just as they had the ALI DBMS.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	Next Generation Core Services Elements (NGCS) **Location Database (LDB)** **LDB Description** A LDB serves as both a legacy ALI database and as a LIS in an i3-compliant NG911 environment. The LDB retains all of the current information, functionality, and interfaces of today's ALI, but also can utilize the new protocols required in an NG911 deployment. The LDB supports the protocols for legacy ALI query and ALI query service, the protocols required to obtain information for wireless calls by querying the mobile positioning center (MPC) or Gateway Mobile Location Center (GMLC), and the protocols required for i3 location information retrieval and conveyance, such as HTTP-Enabled Location Delivery (HELD) or other proprietary protocols. Describe the functionality of the proposed LDB, including additional features and capabilities, error handling, FoCR capabilities, logging and deployment recommendations in detail to address the requirements outlined, with particular attention to the arrangement of the proposed components, user interface, and features, and security aspects.				
NGCS 64	Bidder Response: Bidder Response: NGA 911 is offering Nebraska it's cloud-hosted LDB product as a transitional element to a LIS. The LDB interface portal is available to Originating Service Providers (OSPs) so they can verify that civic addresses will return PSAP or emergency responder URIs either using an Application Program Interface (API) Gateway or through an NGA 911 provided web-based solution from our partner COMsolve. The choice of which method used is determined by the needs and requirements of the OSP. **LDB/LIS**: Exceeding requirements, the LDB/LIS we are providing serves civic addresses and includes support for E911 and i2 as well. These additional features enhance ingress routing for all legacy providers, wireline, wireless and VoIP. The enhanced LDB/LIS covers every scenario for supporting the LNG in the formulation, attachment, and delivery of a valid PIDF-LO compliant Header to the ingress ESRP. For this reason, our LDB/LIS	X			

	maintenance and support interface provides for not only the verification of civic addresses, but also ESRK, ESRD (pANI) for E911, and ESQK for i2. **LDB Initial Load(s):** In preparing the LDB as the routing database for legacy OSPs, locations and keys will initially be ingested in bulk and verified against a data dump from the existing legacy ALI/MSAG/SRDB. Given the diverse sources of this information these loads will not necessarily all be completed at one time. Different parties will be required to verify the data sets relevant for their client records including OSPs, MPC/GMLC's VPC, and other location key and data providers. Verification will depend on the type of service provided whether it is an actual civic address, or a key range. Civic addresses and key ranges are associated with PSAP routing boundaries in the GIS and updated in the LVF validation data prior to being active in the LDB. The process is complete when an input from an OSP or Location Service Provider regularly and uniquely returns the correct emergency responder URI associated with a PSAP endpoint. **Regular LDB Maintenance:** After initial loading, verification and validation, the LDB must be regularly updated by the OSPs and Location Service Providers. NGA 911 offers a number of different options for the LECs to manage their Service Order Input (SOI) Updates. Proper updating requires adherence to a process to ensure data is ingested and the LDB integrity is protected. The OSP sends data to NGA 911 by one of the available ingest methods. The SOI files are loaded into the NGA 911 COMsolve system for processing. The SOI updates validate against the different databases and tables depending on the source and LDB category of the input, if a record passes all validations, the update is applied to the LDB. If the record does not successfully pass all required validations, an error is returned with error codes associated with the specific error type and the update is not applied to the LDB until the error is resolved. **Intuitive Interface (for Web Upload Product:** The COMsolve Web input system automates either single site or batch of the following operations and activities:				

	• **Civic Address management (SOI)** features include add civic address, validate address is resolvable in GIS, update the LVF and activate in the LDB; • **ESRK/ESRD management** features include add ESRK/ESRD range, for ESRD implementations, allocate ESRDs to cell tower, for ESRK implementations - link ESRK range to PSAP and allocate cell tower to appropriate ESRK range, monitor ESRKs/ESRDs level, and warn when ESRK/ESRD levels are low; • **9-1-1 routing table** import updates to routing tables, determine required changes, reassign ESRK Ranges/ESRDs, determine if new 911 trunks are needed, generate LDB list load files to include local address verification function (LVF) pre-check against GIS database where results are made available to OSP, and can be used to update LDB for fixed line applications (ports, adds, disconnects). • **CPE that do not support PIDF-LO:** The properly configured LDB and the resulting PIDF-LO from the LIF can also be used to support an LPG at PSAPs that still use legacy equipment and may require an ALI, E2, or V2 dip for address updating, A similar function will be provided for non i3 SIP based CPE that also require access to an ALI formatted feed.				

Any additional documentation can be inserted here:

The LDB shall meet the following requirements:	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
Shall support all relevant sections of NENA 02-010, 02-011, 02-015, 04-005, 08-501 and 08-502 related to ALI Database Management System (DBMS).	X			
Shall be capable of assuming the role of a location DBMS as defined in NENA-INF-008.2-2013, NENA NG9 1-1 Transition Plan Considerations.	X			
Shall support NENA standards J-036, E2, E2+, non-call-associated signaling (NCAS) and call-associated signaling (CAS).	X			
Shall be able to provide LIS functionality and interfaces as defined in NENA-STA-010.2-2016	X			
Shall be able to seamlessly interact with a NENA i3-compliant ECRF, as described in NENA-STA-010.2-2016.	X			
Shall be able to dereference a location by reference, as defined in NENA-STA-010.2-2016.	X			

Shall be able to dereference requests for additional information, as defined in NENA-STA-010.2-2016.	X			
Shall be able to interface simultaneously with multiple wireless callers.	X			
Shall be able to interface simultaneously with multiple remote ALI databases.	X			
Shall automatically detect, import and validate customer records (SOI records).	X			
Shall have the ability to be used simultaneously by both NG911-capable and E911 capable PSAPs.	X			
Shall allow different PSAPs to use different ALI formats based on individual needs.	X			
Shall utilize LVFs to validate civic addresses.	X			
Shall support PIDF-LO location data formatting as defined in NENA-STA-010.2-2016.	X			
Shall periodically reevaluate the location information using LVF functions within the system.	X			
Shall be able to communicate with NG911 functional elements using the SIP and HELD protocols.	X			
Shall be able to provide a PIDF-LO based on both the wireless and VoIP E2 response.	X			
Shall be able to dereference additional data requests.	X			
Shall consistently respond to all requests within 400 milliseconds (ms).	X			

NGCS 65	**Next Generation Core Services Elements (NGCS)** **Location Database (LDB)** **Integration of Multi-Line Telephone System Data** The LDB shall support the Integration of Multi-Line Telephone System (MLTS) databases. As part of this migration, Contractor shall be responsible for migrating records from the current MLTS databases to the LDB. Provide details on the database migration process and the user interface for management of these MLTS data records.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
	Bidder Response: NGA 911 Legacy 911 Data Migration process will employ validation scripts per noted standards (NENA 71-501, NENA-STA-006.1-2018, NENA-INF-014.1-2015, 3.4.4, DR -20150120_ISF, NENA-REQ-002.1-2016). Overall, via different data interface and migrations the NGA 911 solution supports not only MLTS but all data transitions related to ALI, MSAG including PANI10, LDB, and SOI. Once the ALI is transitioned to the LDB, if the LDB has made the reference to the GIS object, the SI can receive updates of attributes to the LDB mapping. The NGA 911 solution will provide a web interface and/or automated method to provision 9-1-1 to the SI and retrieve post-QA data for the use of maps and/or the computer-aided dispatch (CAD) system.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 66	**Next Generation Core Services Elements (NGCS)** **Discrepancy Reporting** 1. Provide details regarding the proposed solution's report functions for notifying PSAPs any time a discrepancy is detected concerning the BCF, ESRP, PRF, ECRF, LVF, and SI. As part of the detail, explain how a report will be sent for the purpose of reporting the discrepancy to multiple responding PSAPs, as determined by the Commission. Discrepancy reporting is outlined in Section 4.7 of NENA-STA-010.2-2016. 2. Describe the functionality of the proposed discrepancy reporting function in sufficient detail to address the requirements outlined, with particular attention to the user interface and features, and the security aspects.	X			
	Bidder Response: The BCF, ESRP, PRF, ECRF, LVF, and SI discrepancy reports conform to Section 4.7 of STA-010.2-2016, and will notify of discrepancies and include the following information: • Time stamp of discrepancy submittal • Discrepancy report ID • Discrepancy reporting agency domain name • Discrepancy reporting agent user ID • Discrepancy reporting agency contact info • Service or instance in which the discrepancy exists • Additional notes/comments • Discrepancy service or database specifics • Reporting agency's assessment of severity • Location and location validation The response to DR includes the following information: • Responding agency • Responding agent • Responding contact • Estimated response timestamp • Comment • Error code • Validation response Update and error reporting are heavily focused on addresses, roads, and address/roads problems such as:				

- Common problems for address points will include required attributes missing, attribute mismatch with road centerlines, geometry gaps and overlaps, address points out of sequence, parity mismatch, attribute mismatch with polygons, no USPS recognized abbreviations, not in polygons, and duplicated unique IDs within PSAP.
- Common problems for road centerline will include attribute mismatch with polygons, required attributes missing, road centerline in wrong direction, intersection split, address range overlaps, not split at polygons, no USPS recognized abbreviation, not in polygons, and duplicate unique IDs within a PSAP.
- The discrepancy reports comply with RFC 5222 and NENA i3 standards, and capture location, service, location validation, and discrepancy.
- Address and roads data mismatch fixes need to support reconciliation of points where alias and primary names do not match, missing prefixes such as South/S, wrong or missing street types, and spelling errors or differences.
- Discrepancy reports are filed within the following response time standard as being suggested by NENA.

As of NENA i3 v2, only the LVF response time have been codified as detailed below:

Discrepancy Report Resolution

Discrepancy Report	Solution (Busines
LIS validating records against the Location Validation Function (LVF)	3
Spatial Interface (SI) Operator to 9-1-1 Authority on provisioning Geographic Information Systems (GIS) data	3
ECRF/LVF Operator to SI Operator on GIS data provisioning	1
ECRF/LVF Operator to SI Operator on GIS data provisioning	3

LVF Discrepancy Report Review and Resolution
The LVF discrepancy process supports the general management process for all DRs from all aspects of the system and code the DRs for LVF. The DRs should be reviewed on a weekly basis with the management and technical leads for the respective aspects of the LVF. The resolution of the discrepancies should be coordinated with the reporting agency as well as ESInet operational management, then aligned with established change management procedures for data and other configuration items.

A Discrepancy Report (DR) is sent by either NGA 911 or the agency reporting the discrepancy to a responding agency and will pass through several phases:

	• The reporting agency creates the DR and forwards it to the responding agency • The responding agency acknowledges the DR report and provides an estimate of when it will be resolved • The reporting agency may request a status update and receive a response • The responding agency resolves the DR and reports its resolution to the reporting agency NGA 911 through its Web Based Service Dashboard and IMS will make DR reporting available to PEMA and the client agencies so that they can comply with any reporting obligations as defined above and by NENA.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 67	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** PSAPs may have a variety of logging recorders capable of recording SIP traffic and associated media. PSAPs will use the Emergency Call Tracking System (ECaTS) for call logging and capture event details. The Commission will gather statistical data from PSAPs through ECaTS. Describe how the solution interfaces with logging recorders and ECaTS.	X			
	Bidder Response: The NGA 911 solution provides end-to-end performance measurement and analysis. NGA 911 is CHE agnostic and can integrate with the PSAPs CHE and/or accept a serial spill and data dump. In regards to CDR logging and reporting, the NGA 911solution is CHE/CPE agnostic. Our versatile platform easily integrates with any Legacy or Next Generation CHE/CPE system. NGA 911 can easily accept a serial spill via RS 232 or data pump through a network interface. The NGA 911 solution supports a standard NENA serial interface. The physical interface with the NGA 911 system is an EIA connector complying with applicable RS-232 standards in a DB9, DB25 or RJ-11 format. NGA 911 has integrated data into the NGA 911 reporting platform from VESTA, VIPER, WestTel, MicroAutomation, etc. NGA 911 is in the lab with Intrado for testing.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 68	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** **Event Logging Description** Extensive logging of NG911related events, transactions, media, and operations is required. All log entries shall be accurately time-stamped. Logging must include all elements in the call flow including logging of NG911related events within ESInets, the NGCS, the PSAP, and related operations, and is a standardized function used throughout ESInets, NG911 functional elements, and PSAPs. Logged events include ingress and egress to an ESInet, ingress, and egress to a PSAP, all steps involved in call processing, and processing of all forms of media. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: NGA 911 has a logging solution that is capable of extensive logging of NG9-1-1 related events, transactions, media, and operations. NGA 911 can log all entries accurately with a time-stamp. 1. Logging - Standards The NGA 911 Logging system of all ESInet components and NGCS components is compliant with NENA and industry standards. Logs will be maintained for a minimum of 90 calendar days. 2. Log Information The NGA 911 Web-Portal provides access to log information for all ESInet components, the NGCS components and all events that have occurred. It logs and stores historical statistics for network and system events along with the health of the network and event resolution. The NGA 911 Logging Service solution is fully compliant with the NENA Detailed Functional and Interface Standards for the NENA i3 Solution Section 5.13 and NENA-STA-010 section 5.2.2.8. The NGA 911 logging service manages logging information for all devices in the NGA 911 NG9-1-1 network. The Commission and PSAP can access the reports online, by phone, or email. Requests for logs can be made in the following manner				

	• Log in to the portal 24/7/365 and create or request a log • Email our Service team to request a log at Services@nga911.com • Call our service team to request a log 877-899-8337 #2 3. Legal Defensibility NGA 911 understands that logs may be subpoenaed and used as a source of information in legal proceedings. To this end, our system is designed and operated with legal defensibility of logged information. Our system meets, at a minimum, the State Nebraska's requirements for chain of custody, access logs and accurate time stamps. NGA 911 will be responsible for any third-party certification fees necessary to support logging requirements at no cost to the PSAP. NGA 911 logs all elements in the call flow including logging of NG9-1-1 related events within ESInets, the NGCS, the PSAP, and related operations, and is a standardized function used throughout ESInets, NG911 functional elements, and PSAPs. Logged events include ingress and egress to an ESInet, ingress, and egress to a PSAP, all steps involved in call processing, and processing of all forms of media.

Any additional documentation can be inserted here:

Attachment "C"
Option B Revision One
Technical Requirements
Public Service Commission NGCS
Request for Proposal Number 6264 Z1

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 69	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** **Integration with Call-Handling Equipment** 1. Describe how bidder's event-logging solution may integrate with the each PSAP's call-handling equipment, to provide a complete, end-to-end view of a call. 2. Describe how the Commission can gain access to information in the event-logging solution. 3. Describe the requirements of the PSAP's call-handling equipment, software license agreements, and interfaces required to support integration with the bidder's event-logging solution.	X			
	Bidder Response: 1. The NGA 911 event-logging solution is capable of being integrated with the PSAP CPE and is dependent on the cooperation and capabilities of the CPE Vendor's equipment. The NGA 911 solution is CPE agnostic. 2. All authorized State, Commission, and PSAP personnel will have a profile in the NGA 911 Administration Portal to gain access to the event-logging solution to run statistical reports and view Dashboards. The authorized users will have access to canned reports, and client management reports. NGA 911 will provide any needed assistance for running the reports, and support creating custom reports. The credentialed user will log into the NGA 911 web portal using their unique log in. The NGA 911 Self-Service Portal is available 24x7x365 which gives the customer greater reach and flexibility. The Web-Portal is available on a desktop, laptop, tablet, and mobile device. 3. 3. NGA 911 will not require any software licensing agreements. The NGA 911 CHE team will coordinate testing and integration activities with the CAD, recorder, mapping, radio and telco personnel.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 70	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** **Access to Event Logging Data** 1. Describe how the PSAPs and the Commission will gain access via role-based authentication to the event-logging solution data and run statistical and other MIS reports. The PSAP is the custodian of such data for purposes of the Nebraska Public Records Statutes, Neb. Rev. Stat. §§ 84-712 to 84 712.09. The PSAP is responsible for maintaining such data pursuant to the PSAP record-retention schedule applicable to such data as provided in the Nebraska Public Record Statutes, Neb. Rev. Stat. §§ 84 1201 to 84 1229. The state is implementing the ECaTS MIS solution statewide. Upon deployment, the Contractor shall coordinate with ECaTS, the state, and the PSAPs to deliver event logging data to the ECaTS solution. An existing data-sharing agreement (DSA) between the state and the PSAPs governs what data the state may access along with notifications of records requests. This DSA will govern data collected by the NGCS and ESInet provider whether that data is delivered to ECaTS or directly to the state or PSAPs. 2. Describe the reports, MIS tools, and performance metrics made available to each PSAP, the user interface for retrieving or receiving reports, role-based authentication to limit access to data and reports, and the ability to customize reports based on individual PSAP needs. These reports may be used as a basis for changes to bandwidth and capacity. The required reports and metrics will include, but is not limited to: a. Timing b. Call-delivery time c. Call-processing time between elements d. Volumes e. Call volumes by call type f. Alternate-routed calls g. Text-to-911 h. All NGCS element usage volumes i. Bandwidth/trunk utilization j. Calls per trunk k. Trunk utilization l. Circuit utilization	X			
	Bidder Response: 1. Process for Web-Portal access The PSAP appointed Single Point of Contact (SPoC) will provide the NGA 911 Project Manager the following information for each person to have credentials:				

	a. Name, Date of Birth, Email Address, Role, and Jurisdiction where they are allowed access. • The NGA 911 Service Team will build the profile. • The NGA 911 Service Team will provide the login information to the end user. • The NGA 911 Team will provide Admin, Train the Trainer, and End User training. • The PSAP SPoC will update the NGA 911 Service Team of updates, changes, or deletes for authorized credentialed users. NGA 911 will coordinate with ECaTS, the state, and the PSAPs to deliver event logging data to the ECaTS solution. 2. NGA 911 has a full MIS system that can produce canned or ad hoc reports. The system can pull on demand or be set to automatically generate reports and metrics to include, but is not limited to: a. Timing b. Call-delivery time c. Call-processing time between elements d. Volumes e. Call volumes by call type f. Alternate-routed calls g. Text-to-911 h. All NGCS element usage volumes i. Bandwidth/trunk utilization j. Calls per trunk k. Trunk utilization l. Circuit utilization

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 71	**Next Generation Core Services Elements (NGCS)** **Event Logging and Management Information System (MIS)** **NENA Standards Compliance** The bidder's proposed logging solution shall meet the requirements set forth in NENA-STA-010.2-2016. **Third-Party Certification Fees** Bidder is responsible for any third-party certification fees. Describe how the solution meets or exceeds these above requirements.	X			
	Bidder Response: The NGA 911 Web-Portal provides a logging solution to access log information for all ESInet components, the NGCS components and all events that have occurred. It logs and stores historical statistics for network and system events along with the health of the network and event resolution. The NGA 911 Logging Service solution is fully compliant with the NENA Detailed Functional and Interface Standards for the NENA i3 Solution Section 5.13 and NENA-STA-010 section 5.2.2.8. The NGA 911 logging service manages logging information for all devices in the NGA 911 NG9-1-1 network. NGA 911 will be responsible for any third-party certification fees.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 72	**Next Generation Core Services Elements (NGCS)** **Network Time Protocol (NTP) and Time Source** Bidder's solution shall sync with existing time sources to maintain consistent time stamps across the network and systems. Describe how bidder's solution complies with this requirement.	X			
	Bidder Response: System timing is a critical issue for accurate logging. NGA 911's Time Sync Service is fully compliant with the NENA Detailed Functional and Interface Standards for the NENA i3 Solution NENA-STA-010 sections 5.2.2.7 and 5.3.2.4 to maintain consistent time stamps. This service uses a fleet of satellite-connected and atomic reference clocks in each Region to deliver accurate current time readings of the Coordinated Universal Time (UTC) global standard through Network Time Protocol (NTP). The Time Sync Service automatically smooths any leap seconds that are added to UTC. For additional reference (and redundancy), we also connect to the Time Sync Service through NTP at the 169.254.169.123 IP address for any system connected to the NGA 911 ESInet NGCS.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 73	**Next Generation Core Services Elements (NGCS)** **Network Time Protocol (NTP) and Time Source** **Master Clock Description** The bidder shall provide redundant, resilient network-attached Stratum 2 time sources ("master clocks") capable of supplying standard time to all systems, network devices, and functional elements that comprise the ESInet and the NGCS. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: NGA 911 connects to the Time Sync Service through NTP for any system connected to NGCS. This NGA 911 solution provides redundant, resilient network-attached time sources (two (2) master clocks) capable of supplying standard time to all systems, network devices, and functional elements that comprise the ESInet and the NGCS that provide accurate timing with no more than 20 milliseconds (ms) of drift from real time between any device(s).				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 74	**Next Generation Core Services Elements (NGCS)** **Network Time Protocol (NTP) and Time Source** **Accessibility by PSAP Equipment** The master clock time source(s) shall be accessible to the PSAPs for synchronizing call-handling systems and other related systems. All systems, network devices, and functional elements shall support the use of the NTP for maintaining system clock accuracy. Describe how the solution meets or exceeds the above requirements.	X			
	Bidder Response: NGA 911 will make the master clock time source(s) accessible to the PSAPs for synchronizing their call handling systems and other related systems. All systems, network devices, and functional elements proposed by NGA 911 support the use of the Network Time Protocol (NTP) for maintaining system clock accuracy. NGA 911 provides NTP through the Amazon Time Sync Service, time synchronization service delivered over Network Time Protocol (NTP) which uses a fleet of redundant GPS satellite-connected and atomic clocks in each region to deliver a highly accurate reference clock.				

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 75	**Next Generation Core Services Elements (NGCS)** **NG911 Application Integration** Bidder shall describe other NG911 applications, additional data integrations, and personal safety applications that may be integrated with the NGCS solution. The bidder's system must be capable of integration with Additional Data Repositories (ADR), Identity-Searchable Additional Data Repositories (IS-ADR) or commercial third-party LIS, as described in NENA STA-010.2-2016, within two years of the deployment of the first PSAP. Describe how the solution will accomplish integration, information storage, and use/transmission of data to PSAP CHE.	X			

Bidder Response:

Bidder Response:

NGA 911 has taken a leadership role in the promotion and development of EIDO (then EIDD), ADR, and other applications and processes.

1. Developed a means and an API that leverages additional data records (ADR) from numerous sources for use by PSAPs and CPE.
2. Was a leading participant in ICE 7 (the NENA Industry Collaboration Event) where we demonstrated our EIDD and ADR capabilities to the 9-1-1 Industry and our peers. For these efforts we received a commendation from NENA stating that our participation was a key to the success of ICE 7.
3. Continue to develop and enhance EIDO and ADR capabilities in our NGCS as we see increased interest and demand for incident related information collection and dissemination from many of our current and perspective customers.
4. NGA 911 deployed our own LIS which can receive presence information from third-party LIS or LRF (3GPP IMS).
5. NGA 911 already provides in our portal API's capable of being searched and updated with IS-ADR for sensor, heart rate, temperature, environment, and other examples that are accessible by the Call Back Number (CID) and/or P-A-I.
6. Developed an IDX for the efficient exchange of information
7. Is working with leading industries in telematics, alarm and security, telecommunications (i.e. OSPs) and fusion centers to aggregate, evaluate, and deliver incident and relevant additional data to 9-1-1 centers and first responders.

EIDO and IDX

NGA 911 has developed a comprehensive approach to EIDO and IDX in support of proposals to Public Safety Entities and Agencies seeking to integrate EIDO and IDX capabilities into their CONOPs (Concept of Operations). The NGA 911 EIDO being standards based is NIEM conformant – National Information Exchange Model. XML Schema IEPD.

	NGA 911 Incident Management System NGA 911's Incident Management System (NGA-IMS) is a comprehensive suite of tools that support the collection, processing, and presentation of data to the PSAP and First Responders. The NGA-IMS is capable of collecting data from incoming calls, traffic data sources, fusion centers, IOT devices, third party companies (security, information aggregators, telematics, etc) and provide automated and human analysis to prepare an EIDO formatted object for use by our clients. For a particular incident authorized personnel at the PSAP or within First Responder Agencies can access the EIDO, modify, add, edit, and update the Object. Incoming calls are promoted for inclusion in the EIDO if they meet certain criteria as predefined either in CONOPs or as determined by authorities. The diagram below is an overview of how the NGA-IMS makes use of the NGA 911 provided ESInet and NGCS to produce, manage, exchange, update, and distribute EIDOs. NGA 911 will work with the Commission to define EIDO, ADR, and other capabilities to make available in the first two years of the contract and deployment of the first PSAP.

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 76	**Next Generation Core Services Elements (NGCS)** **Message Session Relay Protocol Text (MSRP) Integration** The PSAPs have deployed short messaging service (SMS)-to-911 service. 1. Describe the ability to integrate existing web-based and MSRP-integrated SMS-to-911 and Real-Time Text (RTT) services into the solution. 2. Explain whether the solution supports location-by-reference and/or location-by-value. This requirement is for the integration of text messaging with MSRP and not a requirement for procuring text services.	X			

Bidder Response:

As one of the first NGCS providers to work with Tier 1 wireless operators, NGA 911 further exceeds Nebraska's requirements for implementation of RTT and future services. As a full service, Terminating TCC, Text to 9-1-1 provider our experience is directly relevant to providing statewide Text (and RTT)-to-911 statewide:

1. For Text to 9-1-1 NGA 911 is already a Terminating TCC capable of handling traffic from all of the Wireless OSPs and their designated TCCs. The Terminating TCC is a fully functional MSRP with both web-based and CPE integrated Text-to-9-1-1.

For RTT, NGA 911 is a leader in developing its own standards-based, RTT platform per RFC 4103 and integrating it with Tier 1 Wireless OSPs that are anxious to test this 'new' capability with an existing NGCS provider.

The FCC required the Mobile Network Operators (MNO's) to offer RTT by the end of the year, 2019. NGA 911 was the first NGCS provider to inform all MNOs that we are ready to deploy RTT. This has motivated a number of Wireless OSPs to look to NGA 911 to provide an NGCS to test and qualify their RTT services. This experience puts us in the unique position to address the technical requirements in this section.

Text-to-911(SMS) vs NG Texting services like RTT.

The challenge for 9-1-1 is that SMS is a connectionless unidirectional (like UDP) service that is not suitable for public safety communications. The J-STD-110.01.v002 specification with which we abide by as a Terminating TCC attempts to address this through the adoption of MSRP and other connection-oriented protocols. Although an improvement, the capabilities are significantly limited in comparison to a connection based real time service like RTT. Due to these limitations, basic Text-to-911 is not considered a replacement for TTY. Moreover, the adoption of Text-to-911 in terms of user adoption is atrociously low, at the same time the growth of real time app like Whats App, Telegram, and many others demonstrates that they are fast becoming the major communications platform of this generation. The users of these real time apps are not generally "texting" in that they do not use SMS and are not even aware of its availability to access 9-1-1 service.

	Due to this fact, SMS to 9-1-1 is likely to experience slow growth and will soon be surpassed by RTT and other like services. For this reason, our approach focuses on the future services while being 100% capable of supporting the past with our TCC. Moreover, as a TCC we are able to take even the most advanced RTT based services and deliver text (SMS and MMS) to a less capable device. **Advancing from TCC to NGCS Integrated Service** Whereas SMS-to-911 requires a TCC; NGA 911 integrates RTT directly into our NGCS. As a native service to the NGCS; RTT is integrally tied into whatever additional services may be available through the device – voice, video, voice messages, sensor data, etc. Also implementing Texting as an NGCS service provides all the benefits and call flow control available to other NG communications services to the PSAPs through the PRF. This includes overload handling, PSAP abandonment, and "text" transfers to PSAPs within a region or in neighboring regions. As an integrated service it will also make use of the same interconnections and SD-WAN technology that already exceeds Nebraska's criteria. **2. Location by Reference and Value** NGA 911's NGCS is capable of supporting both Location by Reference and Location by Value. NGA 911's NGCS is capable of receiving Location from Intrado and Commtech for TCC delivery. For RTT, a SIP INVITE with geopriv provides location by reference to the PSAP and/or web-based interface**.**

Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS)	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
	1. Make-Busy Functionality Some PSAPs have a physical make-busy switch that can be activated in the event of an emergency evacuation. Bidder's solution shall support this functionality to all PSAPS.	X			
	2. Ringdown Functionality Bidders' solution shall support ringdown functionality, either through the call-handling system or through the NGCS.	X			
	3. Near-Simultaneous Transfer The solution shall support near-simultaneous conference and transfer capability, with up to at least 12 parties in the conference. This feature shall allow transfer or conference buttons to be programmed to automatically establish a conference with multiple parties. For instance, one button at a police department might establish a conference between the police, fire, and EMS PSAPs and the original caller, without having to add each additional party individually. Describe how bidder's solution meets or exceeds these requirements.	X			

NGCS 77

Bidder Response:

1. Make-Busy Functionality

NGA 911 provides the make-busy capability which we call a 'chicken-switch" for PSAPs to activate in the event of an emergency evacuation. NGA 911 has advanced this capability to allow for more advanced methods to deal with an abandoned PSAP. So whereas we provide this basic make busy, we recommend that authorized users have access to our secure portal that can maintain connectivity to the PRF, NGCS, Dashboard, and Portal to provide more sophisticated routing of calls – to other PSAPs, mobile terminals, and back-up or secondary PSAPs.

2. Ringdown Functionality

NGA 911's NGCS supports ringdown functionality, by using dedicated and preprogrammed lines that are usually integrated into the CPE, but can also be set up as a separate dedicated device that dials automatically when lifted off-hook.

3. Near-Simultaneous Transfer

NGA 911 supports near-simultaneous conference and transfer capability, with up to 20 parties in the conference. Our solution allows transfer or conference buttons to be programmed to automatically establish a conference with multiple parties. These methods are supported by using the REFER, NOTIFY, and SUBSCRIBE bridging functions, but in this case rather than requiring the addition of

	individual parties, a programmed discrete will set up the call immediately with all members being ringed and added as they respond – their SIP address being added to the NOTIFY.

Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS) **PSAP Interfaces and Backroom Equipment Requirements** **Support of PSAP Interfaces** Bidder's solution shall have the ability to support PSAP interfaces specified in NENA STA-010.2-2016, Section 4, including the following: a. SIP calls b. NGCS call delivery c. Web services d. All baseline media and multimedia (as described in NENA STA-010.2-2016, Section 4) e. NTP time services interface, accurate to 1 ms f. Transport layer security g. Discrepancy reporting Describe the functionality of the PSAP interfaces in detail to address the requirements outlined above, with particular attention to the user interface, additional features, and security aspects.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
NGCS 78	Bidder Response: NGA 911 has the ability to support PSAP interfaces specified in NENA STA-010.2-2016, Section 4, including the following **A. SIP Calls** The NGA 911 NGCS is a 100% SIP based infrastructure that adheres to the NENA STA-010.2-2016. All calls presented to the NGA 911 NGCS are SIP signaled. As described below in NGCS Call Delivery, any legacy media, signaling, and support services are converted to SIP and ideally to i3 SIP for presentation to the NGCS. **B. NGCS Call Delivery** NGCS call delivery is based on i3 with any and all necessary legacy accommodations required to support the capabilities (and lack thereof) of the OSPs, the Positioning Centers (location providers), IS-ADRs, the LNG, LPG (if required), the LSRG, and the LDB. The LNG with the PIF, LIF, and NIF as required are called to generate an i3 (or pseudo-i3) INVITE to the ESRP through the BCF. (i.e NGCS Call Delivery mechanism). **C. Web Services**				

NGA 911 is a SOAP compliant NGCS that uses the Service Transport Protocol, XML, SDP (Service Description Protocol and Service Discovery Protocol to provide the HTTP NENA services such as HELD, PIDF-LO, LoST, and NENA NGCS web services.

D. All baseline media and multimedia

NGA 911's all IP system is inherently designed and optimized to handle all baseline media and multimedia. The ESInet and NGCS segments, prioritizes, off loads, compresses, and provides forward error correction (FECs) capabilities which can be programmed and optimized to meet the needs and goals of call takers, PSAPs, host systems, and the Commission.

E. NTP time services interface

NGA 911's Time Sync Service is fully compliant with the NENA Detailed Functional and Interface Standards for the NENA i3 Solution NENA-STA-010 sections 5.2.2.7 and 5.3.2.4. This service uses a fleet of satellite-connected and atomic reference clocks in each Region to deliver accurate current time readings of the Coordinated Universal Time (UTC) global standard through Network Time Protocol (NTP). The Time Sync Service automatically smooths any leap seconds that are added to UTC. We connect to the Time Sync Service through NTP for any system connected to NGCS. Then NGA 911 Time Sync Service can accommodate Central and Mountain time zones. The system shall provide a Time Server on the ESInet using the Network Time Protocol (NTP). PSAPs should use this Time Server to synchronize the clocks on their 9-1-1 CPE, workstations, etc.

F. Transport layer security

The NGA 911 SBC Appliance support SIP over the following protocols: Transmission Control Protocol ("TCP"), User Datagram Protocol ("UDP"), Transport Layer Security ("TLS") over TCP, and Stream Control Transmission Protocol ("SCTP"). These protocols are selectable for each SBC interface to external systems where they are "negotiated" during the initial INVITE directly. Whether through the PCA or a mutually agreed upon Credentialing Authority or mechanism; the certificates are needed in support of TLS (Transport Layer Security) at the BCF. At the border between ESInets a BCF to BCF acting as a B2BUA is established to end-to-end connectivity if required. These provisions will permit interconnections and interoperability with other ESInets. In terms of the NNI for Interoperability, the preferred layer is Layer 3 IP (supporting dual stack IPv4/IPv6). NGA 911 can meet at over 30 locations nationwide to connect and interoperate with every major network operator

	whether a ILEC, CLEC, MSO (cable company), MNO (wireless carrier), or Independent Fiber Company. The table below is a subset of the markets and locations where NGA 911 collocates. **G. Discrepancy reporting** The NGA 911 data and system functionality is managed with Discrepancy Reports that conform to STA-010 and include the following information, but not limited to: • Time stamp of discrepancy submittal • Discrepancy report ID • Discrepancy reporting agency domain name • Discrepancy reporting agent user ID • Discrepancy reporting agency contact info • Service or instance in which the discrepancy exists • Additional notes/comments • Discrepancy service or database specifics • Reporting agency's assessment of severity

Any additional documentation can be inserted here:

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 79	**Next Generation Core Services Elements (NGCS)** **PSAP Interfaces and Backroom Equipment Requirements** **Support of Call Handling Equipment (CHE) Platforms** 1. Provide a list of CHE platforms for which bidder has successfully implemented the interfaces listed above in a live production environment, noting any interfaces that have not yet been tested with each CHE vendor/model. 2. Where interfaces with CHE vendors/models have yet to be deployed and/or tested, please describe the integration testing process that the bidder will perform prior to acceptance testing of the solution. 3. Describe the physical interface handoff required at the PSAP CHE demarcation point.	X			
	Bidder Response: 1. NGA 911 has conducted regular testing and IOT (lab interoperability) testing with the vendors in the table below which lists the interfaces that have been tested and those that have not. Note: NGA 911 is capable of testing all i3 interfaces but most vendors have not deployed a fully functional i3 solution outside the lab at the time of this submission.				

NGA 911 Testbed Status and Functional Test Report

Operational

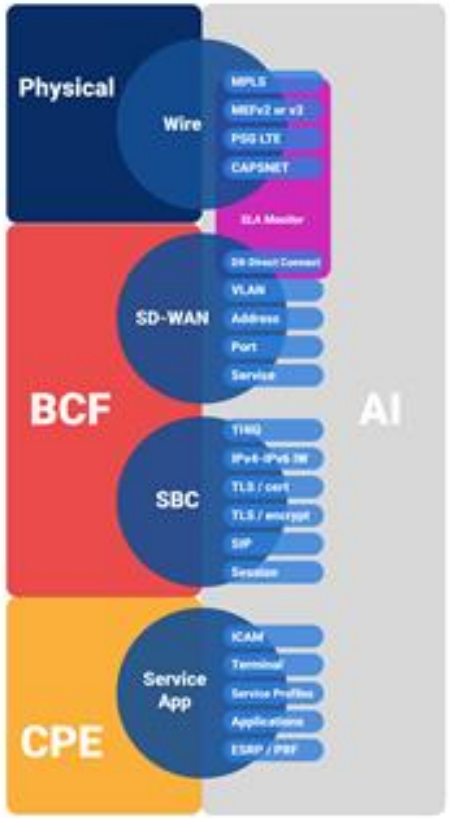
PSAPs				Functional Features Tested							
Organization	**Status**	**Start Date**	**Days**	**Routing**	**SIP Call Delivery**	**NG9-1-1 Call Delivery**	**Geolocation**	**HELD Update**	**Voice**	**RTT**	**Video**
Toronto-Fire PSAP		9/12/2018	628								
Livingston Parish PSAP		1/30/2019	488				CPE-NR	CPE-NR		CPE-NR	CPE-NR
Palo Alto PSAP		1/30/2019	488				CPE-NR	CPE-NR		CPE-NR	CPE-NR
Logan County WV PSAP		1/24/2019	494		CPE-NR	CPE-NR	CPE-NR	CPE-NR	CPE-NR	CPE-NR	CPE-NR
Denco PSAP		1/28/2019	490		CPE-NR	CPE-NR	CPE-NR	CPE-NR	CPE-NR	CPE-NR	CPE-NR
California OES		3/12/2020									

Vendor Test Beds/Labs				Functional Features Tested							
Organization	**Status**	**Start Date**	**Days**	**Routing**	**SIP Call Delivery**	**NG9-1-1 Call Delivery**	**Geolocation**	**HELD Update**	**Voice**	**RTT**	**Video**
		10/16/2018	594							CPE-NR	CPE-NR
		10/9/2018	601							CPE-NR	CPE-NR
		9/12/2018	628					CPE-NR		CPE-NR	CPE-NR
		9/9/2020									
		1/30/2019	488			*	CPE-NR	CPE-NR	CPE-NR	CPE-NR	CPE-NR

CPE-NR = CPE Vendor Not Ready to Test
* Call is Delivered and Received but CPE is not i3 Ready

2. NGA 911 has NDAs with the CPE vendors and cannot reveal the current i3 status of any of them. Both these systems will deploy i3 systems in California in the near future and NGA 911 is the first to test with them.

3. In compliance with i3 NGA 911 will hand-off at the Host/PSAP with a fully compliant NENA BCF as depicted below:



Any additional documentation can be inserted here:

	Next Generation Core Services Elements (NGCS) **Transfer to 7/10-Digit Numbers** The bidder's solution shall be capable of transferring 911 calls to 7 or 10-digit numbers with the Calling Party Number (CPN). Describe how the solution meets or exceeds this requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
NGCS 80	Bidder Response: NGA 911's system supports 9-1-1 Blind and Attended Transfers to 7 or 10- digit numbers with the Calling Party Number (CPN). The selective transfer function is based on a configurable transfer contact database, by PSAP, that includes the list of preferred transfer agency contacts for particular ESN(s) or caller location delivered with the 9-1-1 caller location data (ALI for legacy routing, and caller location for NG9-1-1 routing). The numbers for the preferred transfer agencies can be NG9-1-1 URIs, 7/10-digit numbers, or tandem star code transfer numbers for calls destined for PSAPs connected to the State of Nebraska's ESInet or to PSAP jurisdictions not in the State of Nebraska's ESInet.				

Any additional documentation can be inserted here:

Any additional documentation can be inserted here:

	Service Validation Throughout the life of the contract, upon request of the Commission, Bidder shall allow for network testing and validation by a third-party entity, to verify that the service(s) and/or solution(s) are in compliance with the contract's scope. Describe how the solution meets or exceeds this requirement.	Comply	Partially Comply	Complies with Future Capability	Does Not Comply
		X			
SVAL-1	Bidder Response: NGA 911 will permit throughout the life of the contract, upon request of the Commission, network testing and validation by a third-party entity, to verify that the service(s) and/or solution(s) are in compliance with the contract's scope.				

OPTIONAL SERVICE

		Comply	Partially Comply	Complies with Future Capability	Does Not Comply
NGCS 81	**Next Generation Core Services Elements (NGCS)** **OPTIONAL SERVICES** **NG911 Applications and Alarm Integration** **Alarm Integration Description** NG911 provides for the capability to have alarm companies integrate directly with the ESInet and use the NGCS for routing of the alarm and associated data. Describe bidder's experience with integrating alarms, sensors, and other non-interactive call types with bidder's NGCS solution and include separate pricing.	X			
	Bidder Response: **NG911 Applications and Alarm Integration** **Alarm Integration Description** NG911 provides for the capability to have alarm companies integrate directly with the ESInet and use the NGCS for routing of the alarm and associated data. NGA 911 commits to integrating alarms, sensors, and other non-interactive call types with our NGCS solution. NGA 911 has an extensive lab in which we conduct all testing with vendors such as alarms. NGA 911's team has experience integrating alerting applications into its cloud-based solutions including Safe Kids, an alerting app it developed in 2008. NGA 911's proposed solution is able to accept/integrate with alarm companies, telematic, sensor, and other IoT data into the State of Nebraska's ESInet.				

Any additional documentation can be inserted here:

Instructions To Bidders

General

- All cells are locked except those allowing input (shaded green).
- **Do not attempt to edit formula cells**. Any attempt to edit a formula may cause bidder's entire response to be rejected.
- Tabs will contain cells for Non-Recurring Costs (NRC) and Monthly Recurring Charges (MRC).
- Follow the instructions for each Tab.
- Save as an Excel file and give it a unique name, using the following format: "**Company XYZ XXXX Z1 Cost Proposal Option B NGCS**".
- Print the workbook (not just the worksheets) to verify content of each tab. Also, verify that all data can be seen in each cell.
- Include the saved Excel file when submitting the RFP response package to the Nebraska State Purchasing Bureau.
- Each sheet is divided into the 7 regions. Enter pricing information for each region based on bidders implementation plan.
- All PSAPs and regions may not be ready for geospatial routing on day one of operations and Bidder shall provide tabular routing services, also known as Internet Protocol Selective Routing (IPSR), until such time as PSAPs and regions are ready for geospatial routing. Be sure the cost proposal response indicates the pricing difference between tabular and geospatial routing.
- Include pricing for optional NGCS services on the optional tab.

NRC Milestones

- Milestone Payments - NRC payments will be made as structured on the NRC Milestones Tab.As each region is completed on each tab, it is calculated into the total milestone. **Bidders should prepare their cost proposal to reflect the timeline submitted with Bidder's Implementation Plan.**

Summary Tab

- As the name implies, this tab contains the totals from the **Legacy Network Gateway (LNG)**, **Border Control Function (BCF)**, **Emergency Services Routing Proxy and Policy Routing Function (ESRP & PRF)**, **Emergency Call Routing Function and Location Validation Function (ECRF & LVF)**, **Spatial Interface (SI)**, **Location Database (LDB)** and **Miscellaneous (MISC) tabs.**
- Enter the Bidder name and date in the designated cells. This information automatically populates the other tabs.
- All other cells are locked.

LNG Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Legacy Network Gateway services (hardware, software, connectivity, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the region's population.

BCF Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Border Control Function services (hardware, software, connectivity, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

ESRP & PRF Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Emergency Services Routing Proxy and Policy Routing Function services (hardware, software, connectivity, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

ECRF & LVF Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Emergency Call Routing Function and Location Validation Function services (hardware, software, connectivity, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

SI Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information for Spatial Interface services (hardware, software, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

LDB Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Location Database services (hardware, software, training, maintenance, etc.). Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

MISC Tab

- Change the free form "Bidder Input" labels as needed and enter the pricing information **in each region** for Miscellaneous services that are not part of one of the above functional elements or that may not have been covered in the RFP but are required in order to complete the project. Add rows for each region as needed.
- Enter the NRC in whole dollars and the **MRC in monthly amounts per person amounts in cents**. The monthly amounts are automatically multiplied by 12 and the Region's population.

NGCS Milestones	
Milestone 1: **Region 1** deployments complete	47,250.00
Milestone 2: **Region 2** deployments complete	47,250.00
Milestone 3: **Region 3** deployments complete	47,250.00
Milestone 4: **Region 4** deployments complete	47,250.00
Milestone 5: **Region 5** deployments complete	47,250.00
Milestone 6: **Region 6** deployments complete	47,250.00
Milestone 7: **Region 7** deployments complete	47,250.00
TOTAL	330750.00

6264 Z1 Cost Proposal Option B NGCS Revision One

Bidder Name	NGA 911 LLC
Date (MM/DD/YYYY):	6/3/2020

Next Generation Core Services	**INITIAL CONTRACT PERIOD**														
	YEAR 1		**YEAR 2**		**YEAR 3**		**YEAR 4**		**YEAR 5**		**YEAR 6**	**YEAR 7**	**YEAR 8**	**YEAR 9**	**YEAR 10**
	NRC	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**
LNG	85,000.00	672,754.56	34,000.00	677,768.17	0.00	671,385.26	0.00	671,385.26	0.00	463,024.32	463,024.32	463,024.32	463,024.32	463,024.32	463,024.32
BCF	25,000.00	136,653.27	10,000.00	150,482.90	0.00	150,482.90	0.00	150,482.90	0.00	150,482.90	150,482.90	150,482.90	150,482.90	150,482.90	150,482.90
ESRP & PRF	62,500.00	473,030.55	25,000.00	520,902.36	0.00	520,902.36	0.00	520,902.36	0.00	520,902.36	520,902.36	520,902.36	520,902.36	520,902.36	520,902.36
ECRF & LVF	50,000.00	473,030.55	20,000.00	520,902.36	0.00	520,902.36	0.00	520,902.36	0.00	520,902.36	520,902.36	520,902.36	520,902.36	520,902.36	520,902.36
SI	0.00	10,511.79	0.00	11,575.61	0.00	11,575.61	0.00	11,575.61	0.00	11,575.61	11,575.61	11,575.61	11,575.61	11,575.61	11,575.61
LDB	6,250.00	31,535.37	2,500.00	34,726.82	0.00	34,726.82	0.00	11,575.61	0.00	11,575.61	11,575.61	11,575.61	11,575.61	11,575.61	11,575.61
MISC	7,500.00	10,511.79	3,000.00	11,575.61	0.00	11,575.61	0.00	11,575.61	0.00	11,575.61	11,575.61	11,575.61	11,575.61	11,575.61	11,575.61
Total	236,250.00	1,808,027.88	94,500.00	1,927,933.84	0.00	1,921,550.93	0.00	1,898,399.71	0.00	1,690,038.77	1,690,038.77	1,690,038.77	1,690,038.77	1,690,038.77	1,690,038.77

Project Totals	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
Yearly Totals (NRC+MRC)	$2,044,277.88	$2,022,433.84	$1,921,550.93	$1,898,399.71	$1,690,038.77	$1,690,038.77	$1,690,038.77	$1,690,038.77	$1,690,038.77	$1,690,038.77
Initial Contract (5 Year NRC+MRC)	$9,576,701.12									
+ Optional Year 6 (6 Year NRC+MRC)	$11,266,739.89									
+ Optional Years 7 (7 Year NRC+MRC)	$12,956,778.66									
+ Optional Years 8 (8 Year NRC+MRC)	$14,646,817.43									
+ Optional Years 9 (9 Year NRC+MRC)	$16,336,856.20									
+ Optional Years 10 (10 Year NRC+MRC)	$18,026,894.96									

State Population	
	2019 Estimates
Region One - ~~SE~~ SC	259,183
Region Two - ~~SC~~ SE	512,126
Region Three - Metro	772,006
Region Four - NC	28,227
Region Five - EC	180,423
Region Six - NE	114,203
Region Seven - Metro West	63,100
Total Population	1,670,085

6264 Z1 Cost Proposal Option B NGCS Revision One

Bidder Name:	NGA 911 LLC														
Date (MM/DD/YYYY):	6/3/2020														
	INITIAL CONTRACT PERIOD														
Legacy Network Gateway	**YEAR 1**		**YEAR 2**		**YEAR 3**		**YEAR 4**		**YEAR 5**		**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
	NRC	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**
Region One Milestone															
POIs	5,000.0000	0.0100		0.0090		0.0090		0.0090		0.0050	0.0050	0.0050	0.0050	0.0050	0.0050
SIP Aggregation	2,000.0000	0.0100		0.0100		0.0100		0.0100		0.0100	0.0100	0.0100	0.0100	0.0100	0.0100
LNG	10,000.0000	0.0120		0.0100		0.0100		0.0100		0.0050	0.0050	0.0050	0.0050	0.0050	0.0050
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	17,000.0000	99,526.2720	0.0000	90,195.6840	0.0000	90,195.6840	0.0000	90,195.6840	0.0000	62,203.9200	62,203.9200	62,203.9200	62,203.9200	62,203.9200	62,203.9200
Region Two Milestone															
POIs	5,000.0000	0.0100		0.0090		0.0090		0.0090		0.0050	0.0050	0.0050	0.0050	0.0050	0.0050
SIP Aggregation	2,000.0000	0.0100		0.0100		0.0100		0.0100		0.0100	0.0100	0.0100	0.0100	0.0100	0.0100
LNG	10,000.0000	0.0120		0.0100		0.0100		0.0100		0.0050	0.0050	0.0050	0.0050	0.0050	0.0050
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	17,000.0000	196,656.3840	0.0000	178,219.8480	0.0000	178,219.8480	0.0000	178,219.8480	0.0000	122,910.2400	122,910.2400	122,910.2400	122,910.2400	122,910.2400	122,910.2400
Region Three Milestone															
POIs	5,000.0000	0.0100		0.0090		0.0090		0.0090		0.0050	0.0050	0.0050	0.0050	0.0050	0.0050
SIP Aggregation	2,000.0000	0.0100		0.0100		0.0100		0.0100		0.0100	0.0100	0.0100	0.0100	0.0100	0.0100
LNG	10,000.0000	0.0120		0.0100		0.0100		0.0100		0.0050	0.0050	0.0050	0.0050	0.0050	0.0050
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	17,000.0000	296,450.3040	0.0000	268,658.0880	0.0000	268,658.0880	0.0000	268,658.0880	0.0000	185,281.4400	185,281.4400	185,281.4400	185,281.4400	185,281.4400	185,281.4400
Region Four Milestone															
POIs	5,000.0000	0.0100		0.0090		0.0090		0.0090		0.0050	0.0050	0.0050	0.0050	0.0050	0.0050
SIP Aggregation	2,000.0000	0.0100		0.0100		0.0100		0.0100		0.0100	0.0100	0.0100	0.0100	0.0100	0.0100
LNG	10,000.0000	0.0120		0.0100		0.0100		0.0100		0.0050	0.0050	0.0050	0.0050	0.0050	0.0050
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	17,000.0000	10,839.1680	0.0000	9,822.9960	0.0000	9,822.9960	0.0000	9,822.9960	0.0000	6,774.4800	6,774.4800	6,774.4800	6,774.4800	6,774.4800	6,774.4800
Region Five Milestone															
POIs	5,000.0000	0.0100		0.0090		0.0090		0.0090		0.0050	0.0050	0.0050	0.0050	0.0050	0.0050
SIP Aggregation	2,000.0000	0.0100		0.0100		0.0100		0.0100		0.0100	0.0100	0.0100	0.0100	0.0100	0.0100
LNG	10,000.0000	0.0120		0.0100		0.0100		0.0100		0.0050	0.0050	0.0050	0.0050	0.0050	0.0050
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	17,000.0000	69,282.4320	0.0000	62,787.2040	0.0000	62,787.2040	0.0000	62,787.2040	0.0000	43,301.5200	43,301.5200	43,301.5200	43,301.5200	43,301.5200	43,301.5200
Region Six Milestone															
POIs			5,000.0000	0.0100		0.0090		0.0090		0.0050	0.0050	0.0050	0.0050	0.0050	0.0050
SIP Aggregation			2,000.0000	0.0100		0.0100		0.0100		0.0100	0.0100	0.0100	0.0100	0.0100	0.0100
LNG			10,000.0000	0.0120		0.0100		0.0100		0.0050	0.0050	0.0050	0.0050	0.0050	0.0050
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	0.0000	0.0000	17,000.0000	43,853.9520	0.0000	39,742.6440	0.0000	39,742.6440	0.0000	27,408.7200	27,408.7200	27,408.7200	27,408.7200	27,408.7200	27,408.7200
Region Seven Milestone															
POIs			5,000.0000	0.0100		0.0090		0.0090		0.0050	0.0050	0.0050	0.0050	0.0050	0.0050
SIP Aggregation			2,000.0000	0.0100		0.0100		0.0100		0.0100	0.0100	0.0100	0.0100	0.0100	0.0100
LNG			10,000.0000	0.0120		0.0100		0.0100		0.0050	0.0050	0.0050	0.0050	0.0050	0.0050
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	0.0000	0.0000	17,000.0000	24,230.4000	0.0000	21,958.8000	0.0000	21,958.8000	0.0000	15,144.0000	15,144.0000	15,144.0000	15,144.0000	15,144.0000	15,144.0000
LNG Total	**85,000.0000**	**672,754.5600**	**34,000.0000**	**677,768.1720**	**0.0000**	**671,385.2640**	**0.0000**	**671,385.2640**	**0.0000**	**463,024.3200**	**463,024.3200**	**463,024.3200**	**463,024.3200**	**463,024.3200**	**463,024.3200**

6264 Z1 Cost Proposal Option B NGCS Revision One

Bidder Name:	NGA 911 LLC														
Date (MM/DD/YYYY):	6/3/2020														
	INITIAL CONTRACT PERIOD														
Border Control Function	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone															
BCF	5,000.0000	0.0065		0.0065		0.0065		0.0065		0.0065	0.0065	0.0065	0.0065	0.0065	0.0065
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	5,000.0000	20,216.2740	0.0000	20,216.2740	0.0000	20,216.2740	0.0000	20,216.2740	0.0000	20,216.2740	20,216.2740	20,216.2740	20,216.2740	20,216.2740	20,216.2740
Region Two Milestone															
BCF	5,000.0000	0.0065		0.0065		0.0065		0.0065		0.0065	0.0065	0.0065	0.0065	0.0065	0.0065
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	5,000.0000	39,945.8280	0.0000	39,945.8280	0.0000	39,945.8280	0.0000	39,945.8280	0.0000	39,945.8280	39,945.8280	39,945.8280	39,945.8280	39,945.8280	39,945.8280
Region Three Milestone															
BCF	5,000.0000	0.0065		0.0065		0.0065		0.0065		0.0065	0.0065	0.0065	0.0065	0.0065	0.0065
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	5,000.0000	60,216.4680	0.0000	60,216.4680	0.0000	60,216.4680	0.0000	60,216.4680	0.0000	60,216.4680	60,216.4680	60,216.4680	60,216.4680	60,216.4680	60,216.4680
Region Four Milestone															
BCF	5,000.0000	0.0065		0.0065		0.0065		0.0065		0.0065	0.0065	0.0065	0.0065	0.0065	0.0065
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	5,000.0000	2,201.7060	0.0000	2,201.7060	0.0000	2,201.7060	0.0000	2,201.7060	0.0000	2,201.7060	2,201.7060	2,201.7060	2,201.7060	2,201.7060	2,201.7060
Region Five Milestone															
BCF	5,000.0000	0.0065		0.0065		0.0065		0.0065		0.0065	0.0065	0.0065	0.0065	0.0065	0.0065
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	5,000.0000	14,072.9940	0.0000	14,072.9940	0.0000	14,072.9940	0.0000	14,072.9940	0.0000	14,072.9940	14,072.9940	14,072.9940	14,072.9940	14,072.9940	14,072.9940
Region Six Milestone															
BCF			5,000.0000	0.0065		0.0065		0.0065		0.0065	0.0065	0.0065	0.0065	0.0065	0.0065
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	0.0000	0.0000	5,000.0000	8,907.8340	0.0000	8,907.8340	0.0000	8,907.8340	0.0000	8,907.8340	8,907.8340	8,907.8340	8,907.8340	8,907.8340	8,907.8340
Region Seven Milestone															
BCF			5,000.0000	0.0065		0.0065		0.0065		0.0065	0.0065	0.0065	0.0065	0.0065	0.0065
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	0.0000	0.0000	5,000.0000	4,921.8000	0.0000	4,921.8000	0.0000	4,921.8000	0.0000	4,921.8000	4,921.8000	4,921.8000	4,921.8000	4,921.8000	4,921.8000
BCF Total	**25,000.0000**	**136,653.2700**	**10,000.0000**	**150,482.9040**	**0.0000**	**150,482.9040**	**0.0000**	**150,482.9040**	**0.0000**	**150,482.9040**	**150,482.9040**	**150,482.9040**	**150,482.9040**	**150,482.9040**	**150,482.9040**

6264 Z1 Cost Proposal Option B NGCS Revision One

Bidder Name:	NGA 911 LLC														
Date (MM/DD/YYYY):	6/3/2020														
Emergency Services Routing Proxy & Policy Routing Function	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone															
ESRP & PRF	12,500.0000	0.0225		0.0225		0.0225		0.0225		0.0225	0.0225	0.0225	0.0225	0.0225	0.0225
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	12,500.0000	69,979.4100	0.0000	69,979.4100	0.0000	69,979.4100	0.0000	69,979.4100	0.0000	69,979.4100	69,979.4100	69,979.4100	69,979.4100	69,979.4100	69,979.4100
Region Two Milestone															
ESRP & PRF	12,500.0000	0.0225		0.0225		0.0225		0.0225		0.0225	0.0225	0.0225	0.0225	0.0225	0.0225
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	12,500.0000	138,274.0200	0.0000	138,274.0200	0.0000	138,274.0200	0.0000	138,274.0200	0.0000	138,274.0200	138,274.0200	138,274.0200	138,274.0200	138,274.0200	138,274.0200
Region Three Milestone															
ESRP & PRF	12,500.0000	0.0225		0.0225		0.0225		0.0225		0.0225	0.0225	0.0225	0.0225	0.0225	0.0225
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	12,500.0000	208,441.6200	0.0000	208,441.6200	0.0000	208,441.6200	0.0000	208,441.6200	0.0000	208,441.6200	208,441.6200	208,441.6200	208,441.6200	208,441.6200	208,441.6200
Region Four Milestone															
ESRP & PRF	12,500.0000	0.0225		0.0225		0.0225		0.0225		0.0225	0.0225	0.0225	0.0225	0.0225	0.0225
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	12,500.0000	7,621.2900	0.0000	7,621.2900	0.0000	7,621.2900	0.0000	7,621.2900	0.0000	7,621.2900	7,621.2900	7,621.2900	7,621.2900	7,621.2900	7,621.2900
Region Five Milestone															
ESRP & PRF	12,500.0000	0.0225		0.0225		0.0225		0.0225		0.0225	0.0225	0.0225	0.0225	0.0225	0.0225
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	12,500.0000	48,714.2100	0.0000	48,714.2100	0.0000	48,714.2100	0.0000	48,714.2100	0.0000	48,714.2100	48,714.2100	48,714.2100	48,714.2100	48,714.2100	48,714.2100
Region Six Milestone															
ESRP & PRF			12,500.0000	0.0225		0.0225		0.0225		0.0225	0.0225	0.0225	0.0225	0.0225	0.0225
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	0.0000	0.0000	12,500.0000	30,834.8100	0.0000	30,834.8100	0.0000	30,834.8100	0.0000	30,834.8100	30,834.8100	30,834.8100	30,834.8100	30,834.8100	30,834.8100
Region Seven Milestone															
Bidder Input			12,500.0000	0.0225		0.0225		0.0225		0.0225	0.0225	0.0225	0.0225	0.0225	0.0225
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	0.0000	0.0000	12,500.0000	17,037.0000	0.0000	17,037.0000	0.0000	17,037.0000	0.0000	17,037.0000	17,037.0000	17,037.0000	17,037.0000	17,037.0000	17,037.0000
ESRP & PRF Total	**62,500.0000**	**473,030.5500**	**25,000.0000**	**520,902.3600**	**0.0000**	**520,902.3600**	**0.0000**	**520,902.3600**	**0.0000**	**520,902.3600**	**520,902.3600**	**520,902.3600**	**520,902.3600**	**520,902.3600**	**520,902.3600**

6264 Z1 Cost Proposal Option B NGCS Revision One

Bidder Name:	NGA 911 LLC														
Date (MM/DD/YYYY):	6/3/2020														
Emergency Call Routing Function & Location Validation Function	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone															
ECRF & LVF	10,000.0000	0.0225		0.0225		0.0225		0.0225		0.0225	0.0225	0.0225	0.0225	0.0225	0.0225
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	10,000.0000	69,979.4100	0.0000	69,979.4100	0.0000	69,979.4100	0.0000	69,979.4100	0.0000	69,979.4100	69,979.4100	69,979.4100	69,979.4100	69,979.4100	69,979.4100
Region Two Milestone															
ECRF & LVF	10,000.0000	0.0225		0.0225		0.0225		0.0225		0.0225	0.0225	0.0225	0.0225	0.0225	0.0225
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	10,000.0000	138,274.0200	0.0000	138,274.0200	0.0000	138,274.0200	0.0000	138,274.0200	0.0000	138,274.0200	138,274.0200	138,274.0200	138,274.0200	138,274.0200	138,274.0200
Region Three Milestone															
ECRF & LVF	10,000.0000	0.0225		0.0225		0.0225		0.0225		0.0225	0.0225	0.0225	0.0225	0.0225	0.0225
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	10,000.0000	208,441.6200	0.0000	208,441.6200	0.0000	208,441.6200	0.0000	208,441.6200	0.0000	208,441.6200	208,441.6200	208,441.6200	208,441.6200	208,441.6200	208,441.6200
Region Four Milestone															
ECRF & LVF	10,000.0000	0.0225		0.0225		0.0225		0.0225		0.0225	0.0225	0.0225	0.0225	0.0225	0.0225
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	10,000.0000	7,621.2900	0.0000	7,621.2900	0.0000	7,621.2900	0.0000	7,621.2900	0.0000	7,621.2900	7,621.2900	7,621.2900	7,621.2900	7,621.2900	7,621.2900
Region Five Milestone															
ECRF & LVF	10,000.0000	0.0225		0.0225		0.0225		0.0225		0.0225	0.0225	0.0225	0.0225	0.0225	0.0225
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	10,000.0000	48,714.2100	0.0000	48,714.2100	0.0000	48,714.2100	0.0000	48,714.2100	0.0000	48,714.2100	48,714.2100	48,714.2100	48,714.2100	48,714.2100	48,714.2100
Region Six Milestone															
ECRF & LVF			10,000.0000	0.0225		0.0225		0.0225		0.0225	0.0225	0.0225	0.0225	0.0225	0.0225
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	0.0000	0.0000	10,000.0000	30,834.8100	0.0000	30,834.8100	0.0000	30,834.8100	0.0000	30,834.8100	30,834.8100	30,834.8100	30,834.8100	30,834.8100	30,834.8100
Region Seven Milestone															
ECRF & LVF			10,000.0000	0.0225		0.0225		0.0225		0.0225	0.0225	0.0225	0.0225	0.0225	0.0225
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	0.0000	0.0000	10,000.0000	17,037.0000	0.0000	17,037.0000	0.0000	17,037.0000	0.0000	17,037.0000	17,037.0000	17,037.0000	17,037.0000	17,037.0000	17,037.0000
ECRF & LVF Total	**50,000.0000**	**473,030.5500**	**20,000.0000**	**520,902.3600**	**0.0000**	**520,902.3600**	**0.0000**	**520,902.3600**	**0.0000**	**520,902.3600**	**520,902.3600**	**520,902.3600**	**520,902.3600**	**520,902.3600**	**520,902.3600**

6264 Z1 Cost Proposal Option B NGCS Revision One

Bidder Name:	NGA 911 LLC														
Date (MM/DD/YYYY):	6/3/2020														
Spatial Interface	**INITIAL CONTRACT PERIOD**														
	YEAR 1		**YEAR 2**		**YEAR 3**		**YEAR 4**		**YEAR 5**		**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
	NRC	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**
Region One Milestone															
SI		0.0005		0.0005		0.0005		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	0.0000	1,555.0980	0.0000	1,555.0980	0.0000	1,555.0980	0.0000	1,555.0980	0.0000	1,555.0980	1,555.0980	1,555.0980	1,555.0980	1,555.0980	1,555.0980
Region Two Milestone															
SI		0.0005		0.0005		0.0005		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	0.0000	3,072.7560	0.0000	3,072.7560	0.0000	3,072.7560	0.0000	3,072.7560	0.0000	3,072.7560	3,072.7560	3,072.7560	3,072.7560	3,072.7560	3,072.7560
Region Three Milestone															
SI		0.0005		0.0005		0.0005		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	0.0000	4,632.0360	0.0000	4,632.0360	0.0000	4,632.0360	0.0000	4,632.0360	0.0000	4,632.0360	4,632.0360	4,632.0360	4,632.0360	4,632.0360	4,632.0360
Region Four Milestone															
SI		0.0005		0.0005		0.0005		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	0.0000	169.3620	0.0000	169.3620	0.0000	169.3620	0.0000	169.3620	0.0000	169.3620	169.3620	169.3620	169.3620	169.3620	169.3620
Region Five Milestone															
SI		0.0005		0.0005		0.0005		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	0.0000	1,082.5380	0.0000	1,082.5380	0.0000	1,082.5380	0.0000	1,082.5380	0.0000	1,082.5380	1,082.5380	1,082.5380	1,082.5380	1,082.5380	1,082.5380
Region Six Milestone															
SI				0.0005		0.0005		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	0.0000	0.0000	0.0000	685.2180	0.0000	685.2180	0.0000	685.2180	0.0000	685.2180	685.2180	685.2180	685.2180	685.2180	685.2180
Region Seven Milestone															
SI				0.0005		0.0005		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	0.0000	0.0000	0.0000	378.6000	0.0000	378.6000	0.0000	378.6000	0.0000	378.6000	378.6000	378.6000	378.6000	378.6000	378.6000
SI Total	**0.0000**	**10,511.7900**	**0.0000**	**11,575.6080**	**0.0000**	**11,575.6080**	**0.0000**	**11,575.6080**	**0.0000**	**11,575.6080**	**11,575.6080**	**11,575.6080**	**11,575.6080**	**11,575.6080**	**11,575.6080**

6264 Z1 Cost Proposal Option B NGCS Revision One

Bidder Name:	NGA 911 LLC														
Date (MM/DD/YYYY):	6/3/2020														
Location Database	**INITIAL CONTRACT PERIOD**														
	YEAR 1		**YEAR 2**		**YEAR 3**		**YEAR 4**		**YEAR 5**		**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
	NRC	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**NRC**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**	**MRC[1]**
Region One Milestone															
LDB	1,250.0000	0.0015		0.0015		0.0015		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	1,250.0000	4,665.2940	0.0000	4,665.2940	0.0000	4,665.2940	0.0000	1,555.0980	0.0000	1,555.0980	1,555.0980	1,555.0980	1,555.0980	1,555.0980	1,555.0980
Region Two Milestone															
LDB	1,250.0000	0.0015		0.0015		0.0015		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	1,250.0000	9,218.2680	0.0000	9,218.2680	0.0000	9,218.2680	0.0000	3,072.7560	0.0000	3,072.7560	3,072.7560	3,072.7560	3,072.7560	3,072.7560	3,072.7560
Region Three Milestone															
LDB	1,250.0000	0.0015		0.0015		0.0015		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	1,250.0000	13,896.1080	0.0000	13,896.1080	0.0000	13,896.1080	0.0000	4,632.0360	0.0000	4,632.0360	4,632.0360	4,632.0360	4,632.0360	4,632.0360	4,632.0360
Region Four Milestone															
LDB	1,250.0000	0.0015		0.0015		0.0015		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	1,250.0000	508.0860	0.0000	508.0860	0.0000	508.0860	0.0000	169.3620	0.0000	169.3620	169.3620	169.3620	169.3620	169.3620	169.3620
Region Five Milestone															
LDB	1,250.0000	0.0015		0.0015		0.0015		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	1,250.0000	3,247.6140	0.0000	3,247.6140	0.0000	3,247.6140	0.0000	1,082.5380	0.0000	1,082.5380	1,082.5380	1,082.5380	1,082.5380	1,082.5380	1,082.5380
Region Six Milestone															
LDB			1,250.0000	0.0015		0.0015		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	0.0000	0.0000	1,250.0000	2,055.6540	0.0000	2,055.6540	0.0000	685.2180	0.0000	685.2180	685.2180	685.2180	685.2180	685.2180	685.2180
Region Seven Milestone															
LDB			1,250.0000	0.0015		0.0015		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	0.0000	0.0000	1,250.0000	1,135.8000	0.0000	1,135.8000	0.0000	378.6000	0.0000	378.6000	378.6000	378.6000	378.6000	378.6000	378.6000
LDB Total	**6,250.0000**	**31,535.3700**	**2,500.0000**	**34,726.8240**	**0.0000**	**34,726.8240**	**0.0000**	**11,575.6080**	**0.0000**	**11,575.6080**	**11,575.6080**	**11,575.6080**	**11,575.6080**	**11,575.6080**	**11,575.6080**

6264 Z1 Cost Proposal Option B NGCS Revision One

Bidder Name:	NGA 911 LLC														
Date (MM/DD/YYYY):	6/3/2020														
Miscellaneous	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone															
Alarm Company Integration (by service)	1500.0000	0.0005		0.0005		0.0005		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	1500.0000	1555.0980	0.0000	1555.0980	0.0000	1555.0980	0.0000	1555.0980	0.0000	1555.0980	1555.0980	1555.0980	1555.0980	1555.0980	1555.0980
Region Two Milestone															
Alarm Company Integration (by service)	1500.0000	0.0005		0.0005		0.0005		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	1500.0000	3072.7560	0.0000	3072.7560	0.0000	3072.7560	0.0000	3072.7560	0.0000	3072.7560	3072.7560	3072.7560	3072.7560	3072.7560	3072.7560
Region Three Milestone															
Alarm Company Integration (by service)	1500.0000	0.0005		0.0005		0.0005		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	1500.0000	4632.0360	0.0000	4632.0360	0.0000	4632.0360	0.0000	4632.0360	0.0000	4632.0360	4632.0360	4632.0360	4632.0360	4632.0360	4632.0360
Region Four Milestone															
Alarm Company Integration (by service)	1500.0000	0.0005		0.0005		0.0005		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	1500.0000	169.3620	0.0000	169.3620	0.0000	169.3620	0.0000	169.3620	0.0000	169.3620	169.3620	169.3620	169.3620	169.3620	169.3620
Region Five Milestone															
Alarm Company Integration (by service)	1500.0000	0.0005		0.0005		0.0005		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	1500.0000	1082.5380	0.0000	1082.5380	0.0000	1082.5380	0.0000	1082.5380	0.0000	1082.5380	1082.5380	1082.5380	1082.5380	1082.5380	1082.5380
Region Six Milestone															
Alarm Company Integration (by service)			1500.0000	0.0005		0.0005		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	0.0000	0.0000	1500.0000	685.2180	0.0000	685.2180	0.0000	685.2180	0.0000	685.2180	685.2180	685.2180	685.2180	685.2180	685.2180
Region Seven Milestone															
Alarm Company Integration (by service)			1500.0000	0.0005		0.0005		0.0005		0.0005	0.0005	0.0005	0.0005	0.0005	0.0005
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	0.0000	0.0000	1500.0000	378.6000	0.0000	378.6000	0.0000	378.6000	0.0000	378.6000	378.6000	378.6000	378.6000	378.6000	378.6000
MISC Total	**7500.0000**	**10511.7900**	**3000.0000**	**11575.6080**	**0.0000**	**11575.6080**	**0.0000**	**11575.6080**	**0.0000**	**11575.6080**	**11575.6080**	**11575.6080**	**11575.6080**	**11575.6080**	**11575.6080**

Bidder Name:	NGA 911 LLC
Date (MM/DD/YYYY):	6/3/2020

OPTIONAL NGCS svc.	INITIAL CONTRACT PERIOD														
	YEAR 1		YEAR 2		YEAR 3		YEAR 4		YEAR 5		Year 6	Year 7	Year 8	Year 9	Year 10
	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	NRC	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]	MRC[1]
Region One Milestone				1											
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 1 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Two Milestone															
Bidder Input															
Bidder Input															
Bidder Inpur															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 2 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Three Milestone															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 3 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Four Milestone															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 4 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Five Milestone															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 5 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Six Milestone															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 6 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Region Seven Milestone															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
Bidder Input															
NRC/MRC Region 7 Total	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Optional NGCS svc. Total	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**	**0.0000**

PROJECT DEPLOYMENT PLAN DRAFT

State of Nebraska

Option B

June, 2020
Version 1.0

Table of Contents

1 Document Control 3
2 Introduction 4
2.1 Purpose 4
3 Project Deployment Approach 4
4 Key Personnel 5
5 Project Schedule 6
6 Site Surveys 8
7 Network Requirements and Final Design Solution 8
7.1 Design and Build-Out of Next Generation Core Services (NGCS) 10
7.2 Design and Order NG9-1-1 Trunk Services 10
7.3 Develop and Document Interfaces 10
7.4 Document Database Integration 10
7.5 Dashboard Development 10
7.6 ESInet/IP Network Service Interface 11
8 Phased Installation 11
8.1 Phase 0 – Pre-Planning 11
8.2 Phase I – Planning 12
8.2.1 Phase I – Network Requirements and Final Design Solutions 12
8.2.2 Phase II - Interface and Implementation 13
8.2.2.1 Receive, Create and Verify IP Assignments 14
8.2.2.2 Order, Install, and Test NG9-1-1 Trunks for PSAP 14
8.2.2.3 Activate NG9-1-1 Trunk 15
8.2.2.4 SD-WAN Design & Implementation 15
8.2.3 Phase III Training and Cutover Phase 16
8.2.3.1 NGA 911 Responsibilities during the Cutover 16
8.2.3.2 Training of Staff 17
8.2.4 Phase IV Post Cutover Testing and Support 18
8.2.4.1 NGA 911 Responsibilities during the Post Cutover Testing and Support 18
8.3 Site Requirements 19
8.4 Site Implementation Details 19
8.5 Implementation Verification and Validation 19
9 Technical Support 20
9.1 Tier I technical Support 20
9.2 Incident Management System (IMS) 20

9.2.1 Standard Trouble Response 21
9.2.2 Escalation Matrix 22
9.3 Trouble Ticket Log 23
9.4 Unplanned Downtime, Reason for Outage (RFO) Report, Root Cause Analysis 23
9.5 Service Level Agreement 24
10 Risks and Project Milestones 24
11 Change Management Process 26
Appendix 1: Cutover Plan 28
Appendix 2: Project Milestones Template 33
Appendix 3: NG9-1-1 Functions and Services Acceptance and Authorization Template 34
Appendix 4: Certificate of System Readiness Template 35

1 Document Control

Index	Date	Author(s)	Description	Version
1	6/1/2020	M. Bland	Draft Version	1.0

2 Introduction

2.1 Purpose

The purpose of this document is to detail the implementation and migration strategy for the State of Nebraska's Next Generation Core Services (NGCS). This document describes the phased approach that will be used to address the Public Safety Answering Points (PSAPs) in Nebraska in order to migrate them from the existing legacy network and legacy Selective Routers to a NGCS National Emergency Number Association (NENA) i3 compliant NGCS. The plan outlines the deployment components required to successfully transition from the existing legacy 9-1-1 environment to NGA 911's Next Generation 9-1-1 (NG9-1-1) system.

These include, but not limited to, in aggregate:

- The NGCS including all required components and interfaces.
- ESInet interconnections, NGCS migration, and CPE interoperability.
- NG9-1-1 supporting databases and functions such as Policy Routing Functions (PRF), Business Rules, Location to Service Translation (LoST) and Call Detail Records.
- Coordination with Nebraska for maintenance and support of the Emergency Call Routing Function (ECRF) and associate policy-based routing functions.
- The NOC/SOC, dashboards, and monitoring services required to manage the State and feed data and records to the State of Nebraska and the PSAP.

The plan includes a detailed timeline and milestones for implementation, testing, and deploying all components. In addition, it lists the configuration management, risk management, training, and communication plans and procedures that will be used to ensure an efficient deployment of the components.

3 Project Deployment Approach

This plan concentrates on the technical aspects of implementing the Network Service Provider services that meet NENA NG9-1-1 requirements and standards..

NGA 911 will:

- Provide network NGCS monitoring for the network
- Provide network NGCS performance monitoring
- Provide an Acceptance Test Plan
- Provide a Training Plan
- Provide a Monthly Billing and SLA Plan
- Provide PSAP Cutover Day Plan

4 Key Personnel

Role	Name	Responsibility
Executive Sponsor	Candace Allred	Ms. Allred is responsible for financially authorizing the project and creating the project charter. Ms. Allred will work closely with the project manager (PM). Ms. Allred is accountable to the board: Owns the business case. Keeps the project aligned with the organization's strategy and portfolio direction. She will govern project risk and work with other sponsors.
Project Management and Oversight	Michelle Bland	Ms. Bland will oversee the project as the project director to ensure all tasks are completed. Additionally, Ms. Bland will be your first point of contact for any issues that cannot be resolved by the Project Manager. Ms. Bland was the 9-1-1 Program Manager for the California Highway Patrol for over 10 years. In this position she oversaw 25 communications centers which included troubleshooting, CPE procurement and deployment, building moves, furniture installation, analytic reporting, and administering the wireless program.
Project Manager, PMP	Anne DeGraff	Ms. DeGraff's experience includes over 40 years in the computing and communication fields with over twenty-five years managing complex technical as well as Public Safety projects – Qwest/CenturyLink, Intrado/West Safety Services. Excels in organizing, planning, scheduling and successfully delivering on challenging multi PSAP and vendor deployments. Expertise in Program Management, Project Management, Customer Relations, Strategic Planning and Execution as well as Team Building.
Project Manager	Shelly Guenther	Ms. Guenther has been in project management throughout her career. Ms. Guenther is a recognized leader throughout the telecom industry. As a Project Manager for NGA 911, Ms. Guenther successfully deployed Elko County, NV consisting of 3 PSAPs which transitioned from basic 9-1-1 to NG9-1-1 with a CPE upgrade and GIS component. She also supported both the Logan County, WV and California NG9-1-1 deployments. Ms. Guenter has experience working directly with the PSAP to ensure all tasks, milestones

		are met on time and continued constant communication is had with the PSAP and Stakeholders.
NG9-1-1 NGCS and Trunk Services Coordinator	Miguel Martinez	Primary role will be evaluating the NG Trunks to support State of Nebraska PSAPs. Mr. Martinez will procure and ensure timely installation. Mr. Martinez has been in the 9-1-1 industry for more than 25 years. He has been supporting the PSAP installations and has a superior knowledge of PSAP backrooms, CPE, and connectivity requirements.
CPE Engineer	Roger Nicholls	Lead PSAP backroom Engineer. Mr. Nicholls worked as the lead service technician for Frontier Communications and Verizon for more than 20 years. He has installed and maintained CPE systems for various 9-1-1 CPE platforms.
NG9-1-1 NGCS Services Coordinator	Mike DeWeese	Mr. DeWeese will coordinate OSP aggregation and network cutover plans. Mr. DeWeese has worked with OSPs and the buildout of NG9-1-1 networks for more than 20 years.
NGCS Engineer	Ed Vea	Ed Vea is NGA 911's Chief Technology Officer and lead NG9-1-1 core services engineer
Network Engineer and NOC	Mark LeMonn	Responsible for network monitoring, outage reporting, troubleshooting, liaison with NOC/SOC. Mr. LeMonn has worked in IT and troubleshooting for PSAPs for more than 10 years.

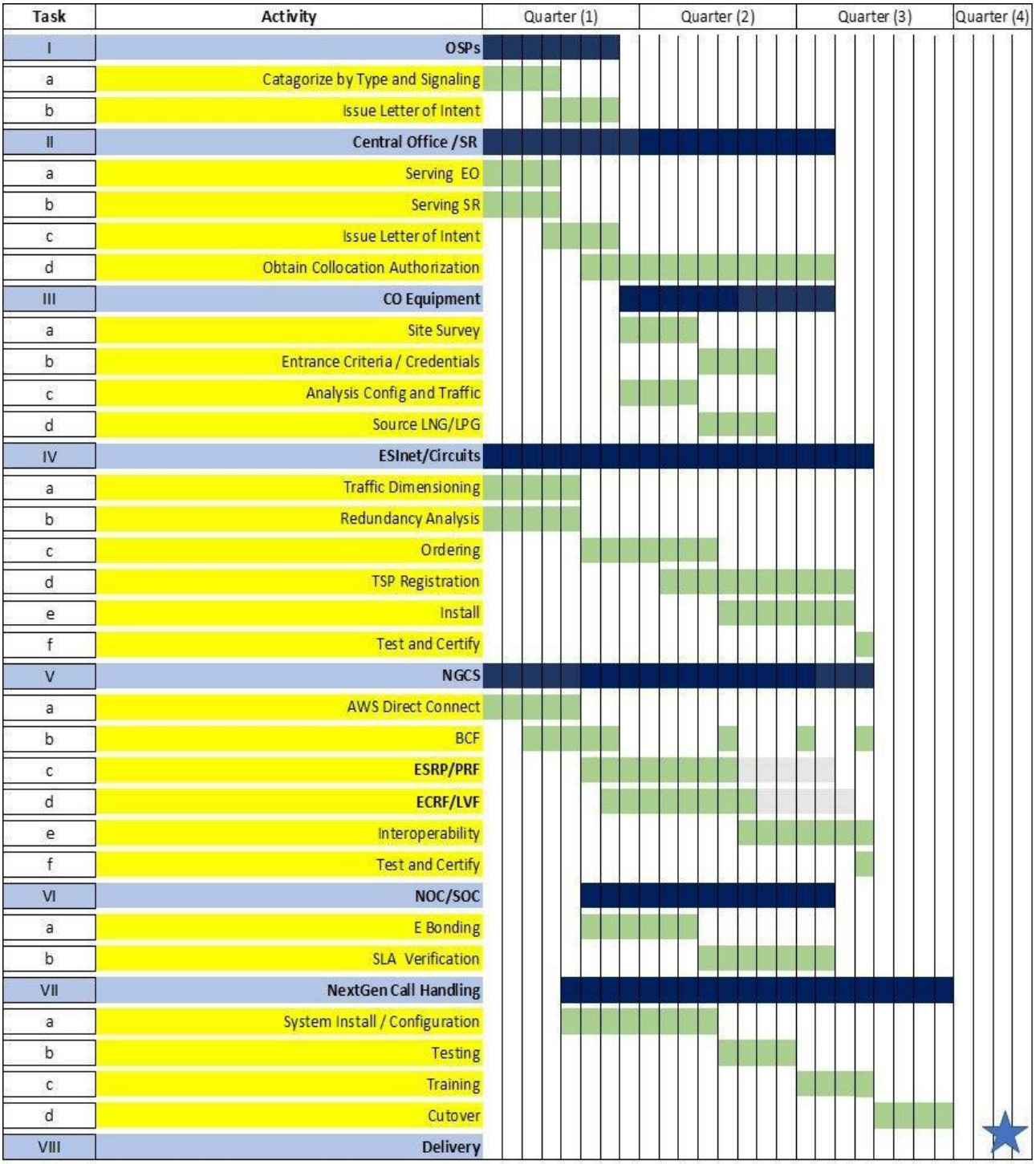
NGA 911 will remove and/or replace Key Personnel for performance under the contract if requested by the State of Nebraska. Key Personnel will not be removed without permission from the State of Nebraska.

5 Project Schedule

A proposed High-Level Project Schedule has been created. The schedule lists the Milestones for the project, along with the steps necessary to complete each of the Milestones listed. The schedule allows NGA 911, as well as the Commission, to monitor the implementation of the project throughout all of the State of Nebraska.

NGA 911 will track the major Milestones with the Smart Sheets schedule and the Project Milestone Reports, required by the Nebraska Public Service Commission, State

9-1-1 Department (Commission). Contract start date is to TBD for purposes of sample timeline a start date is assumed.



6 Site Surveys

External Dependency:

- Approved State Survey Form
- Coordination with the Commission and PSAPs
- PSAP Site Readiness Approval

NGA 911 will complete Site Surveys at each PSAP for Policy Routing Rules and Network Inventory. NGA 911 will coordinate each PSAP site visit with the Commission Project Manager and the PSAP.

NGA 911 will arrive onsite at a predetermined time and date and will use the Site Survey Template provided to the Commission. All findings will be noted on the Site Survey form, along with pictures taken at the PSAP.

NGA 911 will upload all information into the NGA 911 PSAP Database and provide access to the database to the Commission Project Manager as well as provide a soft copy of the completed form, pictures, and a summary report of remediation work required to get the PSAP's site ready for installation and implementation of NG9-1-1.

A priority list will be established based on-Site Survey results. PSAPs requiring additional corrective actions may be moved to a future date based on tasks identified and timeline to complete.

7 Network Requirements and Final Design Solution

External Dependency:

- Interface requirements

The NG9-1-1 System Design includes several key components:

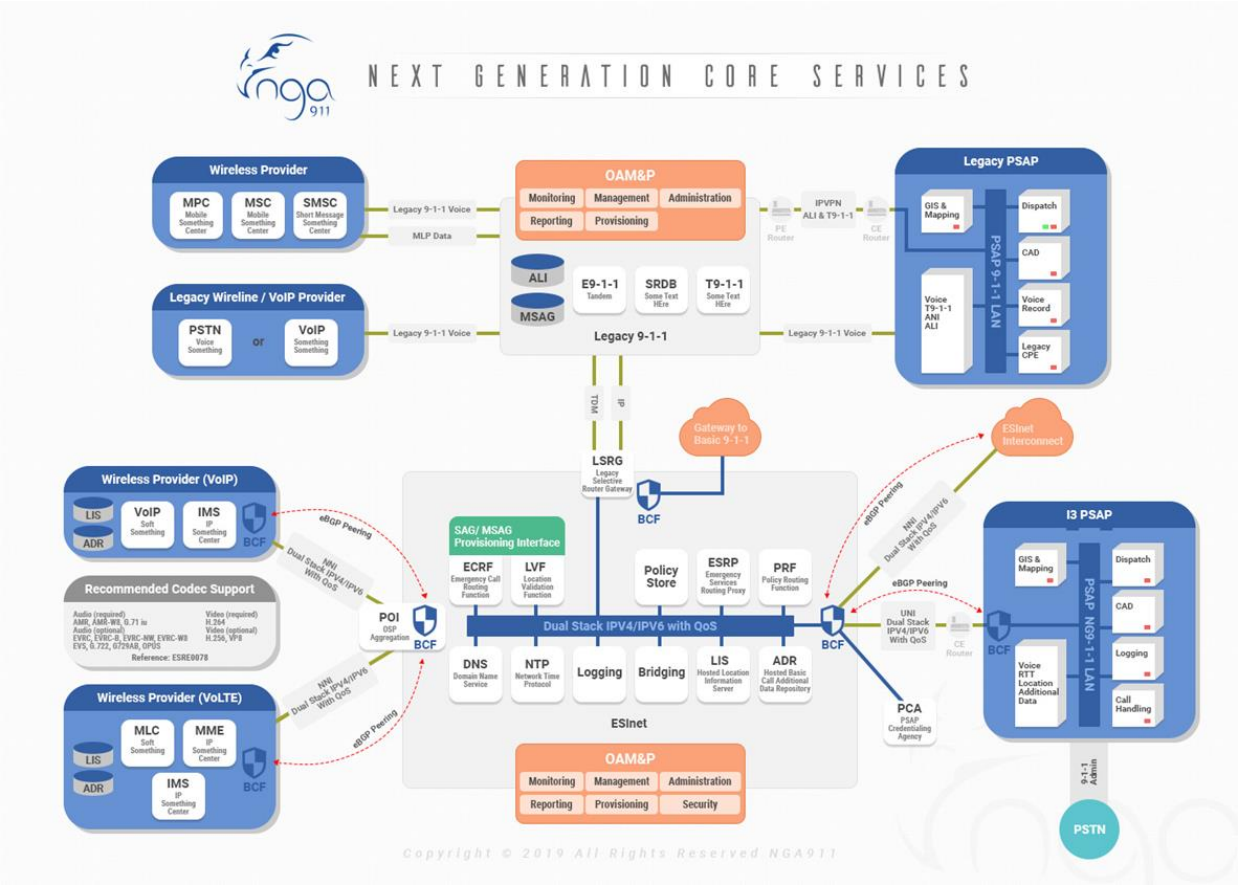
- Call Origination
- IP Access Network
- NG9-1-1 Network
- NG9-1-1 PSAP
- NG9-1-1 Databases

NGA 911's NG9-1-1 design services in the State of Nebraska will follow the National Emergency Number Association (NENA) i3 in NENA-STA-010.2-2016 NENA Detailed Functional and Interface Standards for the NENA i3 Solution. In the standards development process with the Commission, NGA 911 and other providers solutions will be appropriately modified to comply with the new i3 v3 when finalized and within six (6) months of the Commission notification of any future updates to the NENA i3 standard,

at no additional cost to the Commission. NGA 911 will provide an annual compliance report stating how all applicable standards are being met.

Below is the NGA 911 comprehensive NG9-1-1 Function Element diagram covering the elements required from initial transition through to end state.

NETWORK REQUIREMENTS AND FINAL DESIGN SOLUTION			
Letter of Agency (LOA)	7d	9/1/2020	9/8/2020
Finalize Network Design	45d	9/1/2020	10/15/2020
Design and Build NGCS	90d	9/1/2020	12/1/2020
Develop and Document Interfaces	90d	9/1/2020	12/1/2020
Document Database Integration	90d	9/1/2020	12/1/2020
Dashboard Development	90d	9/1/2020	12/1/2020
Establish LNG	90d	9/1/2020	12/1/2020



7.1 Design and Build-Out of Next Generation Core Services (NGCS)
External Dependency: None

NGA 911 will deploy cloud based virtual machines and necessary software in the geo-diverse regions in US West and US East.

7.2 Design and Order NG9-1-1 Trunk Services
External Dependency: None

Identify the access providers, build out connectivity to required locations. Order circuits to maintain diversity to ESInet/datacenter.

7.3 Develop and Document Interfaces
External Dependency: Input from the Commission, PSAP capability

Identify PSAP devices required based on PSAP integration and PSAP capabilities. For instance, whether the PSAP hardware can support i3 call delivery via Session Initiation Protocol (SIP). NGA 911 will develop and build interfaces that are not specified by National Emergency Number Association (NENA) at this time for communication based on the architecture for the Commission, also to include the monitoring and dashboard elements required for the Commission requirement.

7.4 Document Database Integration
External Dependency: Input from the Commission, PSAPs

Determine best method for loading database from OSP and implementing links to Mobile Provisioning Center/VoIP Provisioning Center (MPC/VPC). Working with the Commission to develop update interface and flow down for a database synchronization including LDB and ECRF/LVF updates. NGA 911 will provide independent links to the MPC/VPC infrastructure as part of our national coverage plan.

7.5 Dashboard Development
External Dependencies:

- Input from the Commission

NGA 911 Dashboards are available upon NG9-1-1 trunk installation. NGA 911 will make all fields available to the Commission and provide assistance to identify data of most interest to customize the Dashboard solution to meet the needs of the end user.

7.6 ESInet/IP Network Service Interface

The deployment of the NGCS to the ESInet is not particularly challenging as long as the Commission and NGA 911 are reasonably coordinated. Factors that could have an impact on the project timeline include:

- Designation of data centers and demarcs at all levels.
- Availability and agreement on Credentials, Authorities, and Certificates.
- Underlying Network Service Provider (at Layer 2 and 3) SLA alignment and monitoring.

8 Phased Installation

NGA 911 will deploy the NG9-1-1 system in a phased installation. Using a phased installation allows for several checkpoints during the implementation to confirm that all services are functioning properly and per specification, and to identify and correct any issues that arise.

This approach will start with a proof of concept installation, and then proceed to expand the system and introduce the necessary layers of complexity until the installation is complete. At each milestone, the system and network are tested to demonstrate compliance with the Commission's expectations for functionality and service levels.

8.1 Phase 0 – Pre-Planning

Phase 0 activities ensure that the Project scope has been assessed and that all deliverables are integrated into the Master Schedule.

- Draft Project Milestone Reports and have approved by the Commission
- Develop and Approve the following Plans:
    - Disaster Recovery
    - Project Deployment
    - Installation and Implementation
    - Training
    - Billing
    - Service Level Agreement
- Develop and Approve Site Survey Form and Schedule
- Develop and Approve NG Trunk Installation Provisioning
- Develop and Approve Master Schedule

PHASE 0 PRE-PLANNING			
Disaster Recovery Plan	45d	9/1/2020	10/15/2020
Acceptance Test Plan and Checklist	45d	9/1/2020	10/15/2020
Training Plan	45d	9/1/2020	10/15/2020
Installation and Implementation Plan	45d	9/1/2020	10/15/2020

Maintenance Plan	45d	9/1/2020	10/15/2020
Service Level Agreement Plan	45d	9/1/2020	10/15/2020
Cutover Plan	45d	9/1/2020	10/15/2020
Project Deployment Plan	45d	9/1/2020	10/15/2020
Monthly Billing Plan/Project Milestone Report	45d	9/1/2020	10/15/2020

8.2 Phase I – Planning

Phase I activities ensure that the Project scope has been assessed and that all deliverables are integrated into the Master Schedule.

- Site Survey Form Approval
- Submit Site Survey schedule for Review
- Master Schedule Approval
- NG Trunk Design Approval

PHASE I PLANNING			
Site Survey Form Approval	7d	9/18/2020	9/25/2020
Submit Site Survey schedule for Review	7d	9/25/2020	10/2/2020
The State reviews/approves Site Survey Schedule	3d	10/5/2020	10/7/2020
Master Schedule Approval	3d	10/7/2020	10/10/2020
NG Trunk Design Approval	45d	9/1/2020	10/15/2020
PSAP Remediation			
Draft Project Milestone Reports and have approved by the Commission	7d	9/14/2020	9/21/2020
Perform Site Surveys	30d	10/7/2020	11/7/2020
Review Work Order with PSAP	37d	10/7/2020	11/13/2020
PSAP Backroom Remediation	37d	10/7/2020	11/13/2020
PSAP Site Readiness Approval	37d	10/7/2020	11/13/2020

8.2.1 Phase I – Network Requirements and Final Design Solutions

Phase I activities ensure that the Project scope has been assessed and that all deliverables are integrated into the Master Schedule.

- Develop and Approve Master Schedule. Letter of Agency (LOA)
- Finalize Network Circuit Design
- Design and Order NG9-1-1 Trunk Services
- Design and Build NGCS
- Develop and Document Interfaces
- Document Database Integration
- Dashboard Development
- ESInet Connectivity Design

- Order Materials
- Validate trunk count w/OSPs and other carriers
- Establish POI
- Establish LNG

NETWORK REQUIREMENTS AND FINAL DESIGN SOLUTION			
Letter of Agency (LOA)	7d	9/1/2020	9/8/2020
Finalize Network Circuit Design	45d	9/1/2020	10/15/2020
Design POI and ESInet Connectivity Points	60d	9/1/2020	11/1/2020
Design and Build NGCS	90d	9/1/2020	12/1/2020
Develop and Document Interfaces	90d	9/1/2020	12/1/2020
Document Database Integration	90d	9/1/2020	12/1/2020
Dashboard Development	90d	9/1/2020	12/1/2020
Circuit Connectivity to PSAPs	90d	9/1/2020	12/1/2020
Design SD-WAN Install and Routers	90d	9/1/2020	12/1/2020
Establish LNG	90d	9/1/2020	12/1/2020

8.2.2 Phase II - Interface and Implementation

Phase II is the time in which site implementation take place. The project's implementation is accomplished to the degree that is possible without actually going live while minimizing disruption of the site's ongoing operations. Implementation milestones are deliverables that will be documented and managed in the Master Project Schedule.

Installation and Implementation include:

- NG Trunks (ESInet)
  - Orders are placed
  - Due dates are established
  - Installation is complete
  - Tested and Accepted
- SD-WAN
  - Hardware installed
  - Powered up and connected to NOC
  - Configurations updated
  - Monitoring commences
  - PSAP link(s) accepted (as installed)
- IP Assignments
  - Establish logical address assignment (IPv6) based on mutually agreed upon design terms

The Implementation Phase ends when:

- Finalize PSAP list with the Commission for cutover design

- ID Logical Network Addresses
- PSAP Connectivity
- Deliver and Test Circuits to ESInet
- Design, Implement, and Test SD-WAN
- NG9-1-1 NGCS
- NG9-1-1 Functional Element Provisioning
- NG9-1-1 Connectivity
- Test NG9-1-1 Solution

At the conclusion of the site's implementation process, a system freeze will be announced. This freeze is projected to be 48 hours prior to actual cut date. During Phase II, the site freeze will be scheduled in the Master Project Schedule.

PHASE II INTERFACE AND IMPLEMENTATION			
Finalize the State for Cutover Design	60d	11/1/2020	1/1/2021
ID Logical Network Addresses	7d	12/1/2020	12/8/2020
Test Circuits to ESInet	90d	10/1/2020	1/1/2021
Implement and Test SD-WAN	90d	10/1/2020	1/1/2021
NG9-1-1 NGCS	90d	12/1/2020	3/1/2021
NG9-1-1 Functional Element Provisioning	90d	12/1/2020	3/1/2021
NG9-1-1 Connectivity	90d	12/1/2020	3/1/2021
Test NG9-1-1 NGCS Solution	120d	1/1/2021	4/30/2021

8.2.2.1 Receive, Create and Verify IP Assignments

NGA 911 will establish logical address assignment, IPv4/IPv6 based on mutually agreed upon design. Based on these design terms, NGA 911 will create a record for the deployment of the State of Nebraska, WAN assignments will be ordered with the NG9-1-1 trunk services that will contain the routing and blocks associated with each specific site.

8.2.2.2 Order, Install, and Test NG9-1-1 Trunks for PSAP

Upon completion of the site surveys and an evaluation of available Local Exchange Carrier (LEC) and 3rd party providers, the NGA 911 team will place all NG9-1-1 Trunk orders ESInet and Data Centers for the State of Nebraska. The orders will be placed in the same priority order as the site surveys were completed. NG9-1-1 Trunk Orders will be tracked to their completion by NGA 911 personnel in our circuit provisioning team. A formal notice of circuit installation completion will be sent to the end customer once a circuit has been successfully installed, tested for Layer 2 connectivity, and is ready for use. We will also track completion of each site and report our progress to the Commission in our weekly status meetings.

8.2.2.3 Activate NG9-1-1 Trunk

The NGA 911 NG9-1-1 Trunk Services Coordinator will schedule and be the point of contact to facilitate the NG9-1-1 Trunk installation to the ESInet in the State of Nebraska while providing updates to the NGA 911 Project Manager. The NGA 911 NG9-1-1 Trunk Services Coordinator will also work with the NGA 911 NGCS Coordinator to schedule NG9-1-1 Trunk turn-ups at each of the PSAP's and Data Centers. All work will be coordinated between the NGA 911 Project Manager and the Commission's Project Manager.

- Network Services Connectivity Confirmation: NG9-1-1 Trunk Services Coordinator verifies that the network is deployed to each defined location on a "location-by-location" basis. From this confirmation, a dispatch will lead to installation of extended demarcation wiring and associated hardware to the location identified during the site survey.
- Turn-up Network Services: Activation of the network to the edge device, confirmation of Internet Control Messaging Protocol (ICMP) connectivity to the NGA 911 Edge router or SD-WAN endpoint.
- Test Network Services: Validation of routing and throughput to the NGCS locations from each diverse circuit.

8.2.2.4 SD-WAN Design & Implementation

The NGA 911 Trunks Services Coordinator will coordinate and oversee the order placement. The NGA 911 Project Manager will ensure site readiness and handoff the project to an NGA 911 SD-WAN Project Manager (PM) once IP's are assigned. The NGA 911SD-WAN PM will coordinate all installation activities and oversee related work to completion.

SD-WAN design and implementation is contingent on the IP address information availability provided from the transport circuits.

The NGA 911 Chief Technology Officer will perform data collection prior to the design, which will include Network Design and an SD-WAN Statement of Work. The NGA 911 SD-WAN PM will coordinate design discussions with the Technical Design Engineer when the order progresses to that point.

The NGA 911 SD-WAN PM will coordinate device staging and shipment, customer provided network details, and activation configuration loaded into the directory.

The NGA 911 SD-WAN PM will coordinate SD-WAN Activation with the NGA 911 Core Services PM and provide a Contingency Activation Failure plan.

The Deployment schedule will be based on the customer's site priority and any design specifications (EX: Hub/Spoke topology). There is a 2-stage activation per site.

- Stage 1 will establish connectivity of the transports through the SD-WAN device, testing to confirm there are no issues
- Stage 2 will push all network traffic through the SD-WAN device. Standard testing will be conducted by the activation engineer with support given to the customer on any special/additional testing requests

8.2.3 Phase III Training and Cutover Phase

The Cutover Plan defines the sequenced procedures and steps that will occur in the Site Cutover Phase to bring new equipment to an operational state, as well to transition services from the old legacy network to the new ESInet NGCS.

The Cutover Phase is the major transition point for the project. The Installation and Implementation Plan will specify specific tasks and responsibilities for NGA 911 provided systems, materials, and services. The Cutover Phase will be scheduled in the Master Project Schedule, and conducted as per a site-specific cutover schedule that will be developed during the overall project planning phase and incorporated into the Project Plan. See site specific Cutover Plan Sample Appendix 1.

- PSAP Training
- PSAP Cutover

PHASE III - TRAINING AND CUTOVER			
PSAP Training (Per PSAP)	3d	6/1/2021	6/4/2021
PSAP Cutover (Per PSAP)	3d	6/10/2021	6/12/2021

*PSAP cutover anticipated to begin June 10, 2021 and complete by June 12, 2021. Cutover duration is measured in days per PSAP.

At a high level, the State of Nebraska PSAPs will have all NG9-1-1 infrastructure and equipment in place, tested and accepted to the NGA 911 NGCS. The NGA 911 Aggregation Coordinator will establish a cutover date, time and host a bridge to coordinate OSP translations that will transition calls from the legacy network to the NGA 911 NGCS.

8.2.3.1 NGA 911 Responsibilities during the Cutover

The NGA 911 Project Manager will coordinate assignment of appropriate technical staff to support the transition to the State of Nebraska NGCS. Resource assignments will be planned and tracked in the Master Project Schedule.

- Pre-cut and Post-cut site testing will be performed in accordance with the NGA 911 Verification Checklists that will be shared with the Commission
- Track issues and/or exceptions noted during the site cutover using an Issue Control Log

- Develop Recovery Plan. Should site cutover be interrupted or if any problems or issues arise that may postpone the process, the cutover will be stopped, and existing 9-1-1 trunks will be put back into service until issues are resolved

The Cutover and Training Phase ends when:

- The site training is complete to the degree the end users can operate the system
- Cutover testing is complete

8.2.3.2 Training of Staff

NGA 911 will provide qualified instructors to cover all aspects of the NGCS. NGA 911 will conduct the training as close to the installation date as practical and be in concert with the scheduling needs of the centers and IT staff, if appropriate. The Commission will have the right to replace the instructor.

Training will be provided to the Commission so they will understand the components of our solution at the PSAP's designation. NGA 911 will conduct initial training upon migration.

All newly hired employees will have access to hard, soft and recorded trainings of the NGCS system available on the Web 24x7x365. NGA 911 will also provide continued support and resources.

SESSION ONE ADMINISTRATION AND REPORTING PORTAL - ONE (1) HOUR ON SITE TRAINING THAT WILL BE RECORDED FOR WEB-BASED TRAINING CURRICULUM:

- Web User Trouble Reporting Interface Overview
- Network/Monitoring/Help Desk Web Interface
- Admin Training Module
- Train the Trainer Module
- Service Monitoring Tools
- Help Desk 877-899-8337 press #2
- Canned and custom Management Information System (MIS) reports
- Set up automatic reports

NGA 911 CONTINUED SUPPORT FOR SUCCESS RESOURCES:

- Online Resources including video training and tutorials
- Web User Interface Overview
- Reporting - Management Information System
- Teleconferences
- Webinars
- Training PowerPoints
- Support telephone number for the Commission and the PSAPs
- Maintenance and system(s) support training

8.2.4 Phase IV Post Cutover Testing and Support

The Post cut Testing and Support Phase shall begin with the conclusion of the PSAP's cutover and continues for 30 days. Its purpose is to provide immediate technical support.

The Post cut Testing and Support Phase consists of:

- Commencement of 1st Level Support by NGA 911
- Engineering Support
- Completion of product specific site verification test forms
- Exceptions reporting and action planning

PHASE IV POST CUTOVER AND SUPPORT			
Network Monitoring	On going	On Going	On Going
Monthly Reports	On going	Monthly	On Going
Monthly User Meeting	On going	Monthly	On Going
Annual face-to-face Meeting	On going	Annually	On Going

*Network Monitoring is for the life of the contract

8.2.4.1 NGA 911 Responsibilities during the Post Cutover Testing and Support

The NGA 911 Project Manager will host a Post Cutover Meeting within 30 days following a site cutover. The Project Manager responsibilities during Post cut Testing and Support will include:

- Review the project implementation, open issues, and discuss ways to improve the overall implementation process.
- Ensure that NGA 911 technical support are available to the PSAP in the 24 hours preceding the conclusion of the site cut.
- Complete all site testing material and turnover to the Commission.
- Gain consensus from the Commission that all NGA 911 deliverables as outlined in the approved Project Plan have been met.
- Note any exceptions and generate an action plan to address and correct all remaining issues.
- Report or escalate any maintenance issues.

NGA 911 is customer care focused and strives to continually improve our services and support for our customers. The Post Cutover process allows NGA 911 to collect feedback from the Commission and improve processes.

8.3 Site Requirements

NGA 911 is dependent on the Commission for the following data but not limited to the following list:

1) Point of Contact for the project.
2) The definitive addresses and contact information for all participating PSAPs by County.
3) List of County Coordinators with contact information.
4) List of CPE deployed at each PSAP:
    a. By vendor, model, version
    b. Current upgrade status and timeline
    c. Product representative contact information
5) The ANI/ALI and MSAG data and maintenance providers.
6) Access, as needed, to circuit diagrams, facility and electrical plans and drawings for all PSAPs, government and leased facilities used by 9-1-1 in the State of Nebraska that will be impacted, adapted, enhanced, or connected to NG9-1-1 through the term of the agreement.
7) Access to any Governance materials and agreements such as Memorandum of Understanding (MOU) at the Commission, regional, municipal, and local levels that impact 9-1-1 operations and performance in the State of Nebraska.
8) Other materials, resources, and information in the possession of the Commission and/or state and municipal entities as needed and relevant to the performance of the contract.

8.4 Site Implementation Details

For each PSAP, NGA 911 will provide their deployment plan information 20 calendar days before the PSAP installation or a mutually agreed upon date. The deployment plan shall include, but not limited to:

a) PSAP training
b) Admin training if applicable
c) Go Live Date
d) PSAP name and contact

8.5 Implementation Verification and Validation

The NGA 911 proposed NG9-1-1 System test plan includes, but not be limited to testing for:

- NENA-STA-010.2-2016 functional element testing
- 9-1-1 call flow, primary, alternate and last route options
- ESInet throughput and capacity testing to NGCS
- ESInet end to end connectivity testing to NGCS
- Fault tolerance testing
- ESInet failover and alternate route testing with NGCS
- NGCS monitoring systems

- Fault notification
- Firewalls, intrusion detection systems, intrusion protection systems

9 Technical Support

NGA 911 maintains an Incident Management System (IMS). The IMS generates an incident that remains open and in queue until it is resolved. Once a PSAP/Commission notifies NGA 911 of an issue, they will be provided a unique incident number, date and time opened, status of the ticket, and description of the problem reported via email, if available, or by voice. All notes regarding troubleshooting and/or research performed are documented in the notes field and are readily available to the customer. Each incident is assigned a priority level and updates or changes to the priority level are automatically entered in the tracking log with the user ID of the individual making the change along with a timestamp. Additionally, the NGA 911 Trouble Ticketing System allows the customer to pull their reports of open and closed incidents via an online portal. NGA 911 exceeds with our IMS that automatically sends email updates to members whenever a change is made to the incident including all notes made to the tracking log, priority level changes, and incident closure. Additionally, a Technical Service Representative will be assigned to monitor, and notification the member via telephone with updates.

9.1 Tier I technical Support

Tier I Technical Support is managed by the NGA 911 Help Desk 24x7x365 and is available to the Commission and all PSAPs for technical services support for all products and services included in contract. The Commission and PSAPs can obtain information, updates, and status of service issues, account information, including but not limited to help with the reporting system. The Commission and PSAPs may request assistance or report trouble in three ways:

1. By dialing 1-877-899-8337; Option 2 and report trouble directly to the Help Desk.
2. By sending an email to Support@NGA911.com
3. Via Administrative Web Portal by accessing the Incident Management System (IMS) via the NGA 911 Dashboard.

The NGA 911 Help Desk does not use an automated attendant or other automated means. The Help Desk has the ability to communicate directly and immediately with maintenance and support services for the NGA 911 solution proposed system and all components of the proposed system including without limitation, network trouble. The Help Desk also has access to Executive Management if needed for assistance.

9.2 Incident Management System (IMS)

The NGA 911 IMS is a web-based solution that is easy to use. The IMS generates an incident that remains open and in queue until it is resolved. The NGA 911 IMS allows for incident management capabilities for trouble ticket management. It keeps a log of

troubleshooting and/or research performed along with support requests from the Commission, end users, PSAPs, and ones the system automatically generates. The Self-Service Portal is available 24x7x365 which gives the customer greater reach and flexibility. The customer can submit and check the status of incidents, view notes and history as well as run reports as needed.

The authorized users will be able to view open, resolved, and pending tickets along with the details in each ticket.

9.2.1 Standard Trouble Response

NGA 911's standard response to trouble reports is as follows:

a) Emails: Two hours or less.
b) Calls to Help Desk: Immediate answer.
c) Submission through the IMS.
d) The designee will receive an immediate email confirmation of trouble report created.
e) The designee will receive an email response confirming NGA 911 is processing the trouble ticket outlining next steps. The time lapse between receipt of trouble submission and NGA 911 response will be based upon the Customer indicated priority level. However, all submissions will receive a response no later than 30 minutes from the time of submission.

NGA 911 has clearly defined processes that include an Escalation Matrix, Prioritization, and Incident Handling protocols.

Severity Level 1: Critical Impact/System down

Examples including but not limited to:

- The entire system, or an entire subsystem failure
- Network failure to the PSAP
- Any factor that prevents call movement at ingress or egress
- Catastrophic Building fault e.g. flooding

Response Time: Initial response is under 30 minutes (any time of day). Problem will be addressed hourly until the system is restored to a functional and mutually agreeable state pending a permanent fix. If a catastrophic (hardware or software) fault is found with the equipment/system, this correction will be addressed immediately. NGA 911 will provide a correction for software or hardware (Replacement, Replace, or Recall) as required to restore the system to operation.

Severity Level 2: Significant Impact

Examples including but not limited to:

- Occasional service interruptions
- System operations can be recovered by manual intervention
- Major system features or functions are affected

- A redundant component failure but system is operational

Response Time: Initial response under 30 minutes (any time of day). Problem will be addressed every 2 hours/per day until the system is restored to a functional and mutually agreeable state pending a permanent fix.

Severity Level 3: Normal/Minor Impact
Examples including but not limited to:
- The failure restricts use of a capability
- Non-critical function affected

A redundant part of the hardware or software has failed, and the system is still operating completely, however, without backup.

Response Time: This level of severity will be addressed in 8 hours. If a maintenance software release, or a hardware bulletin to address this issue the ticket may not be resolved in 48 hours. Any new features the Customer may request will be addressed individually outside of this agreement.

Severity Level 4: Low/Informational
Examples including but not limited to:

- The failure results in an acceptable workload
- Prevents or restricts use of a non-essential capability and can be handled procedurally
- Product enhancement not service affecting

Response Time: This level of severity will be addressed within 96 hours during business hours. A technical bulletin may result. Any new features the Customer may request will be addressed individually outside of this agreement.

9.2.2 Escalation Matrix
The NGA 911 processes ensure all team members are clear on the proper protocol and channels for escalation which ensures rapid triage of all incidents. In addition to service response and service resolution, the escalation matrix helps ensure that the available resources are focused on problems that severely affect service. This table defines when additional resources are notified to ensure management is aware of problems and can provide troubleshooting support:

Elapsed Time	Severity Level 1	Severity Level 2	Severity Level 3	Severity Level 4
5 minutes	Network operations manager, Chief Technology Officer, Senior VP Operations			

1 hour	Update to network operations manager, Chief Technology Officer, Chief Executive Officer, Senior VP Operations	Update to network operations manager, Chief Technology Officer, Chief Executive Officer, Senior VP Operations		
2 hours	Escalate to CEO, update to director, operations manager			
4 hours	Root cause analysis to VP, Network operations manager, Chief Technology Officer, Senior VP Operations, unresolved requires CEO notification	Escalate to CEO, Root cause analysis to VP, Network operations manager, Chief Technology Officer, Senior VP Operations, unresolved requires CEO notification		
24 hours			Network operations manager	
5 days				Network operations manager

9.3 Trouble Ticket Log

The IMS maintains a Trouble Ticket Log that tracks the progress and status of restoration for all applicable Service Level Agreements (SLAs). The Trouble Ticket Log is accessible through the Self-Service Portal 24x7x365. The Trouble Ticket Log includes:

- Date and time that each failure was reported
- System/service alarm of failure
- Each PSAP affected by the failure
- Current status of the restoration process
- Date and time the failure is remedied

9.4 Unplanned Downtime, Reason for Outage (RFO) Report, Root Cause Analysis

In the event an individual NGCS component is impacted by unplanned downtime or an outage occurs, NGA 911 will provide, at the request of the Commission and/or PSAP, a written disclosure statement within the agreed upon timeframe via email which will include but not limited to:

1) The component that failed.
2) The duration the component was impacted.
3) Impact to the overall service due to the component failure – including impacted PSAP(s) by FCC Identification (ID).
4) Corrective action taken to recover the component.

In addition to the above disclosure, NGA 911 will provide a RFO report to the Commission and affected PSAPs no later than three calendar days after discovering the outage. NGA 911 will provide an initial root cause analysis no later than ten calendar days after discovering the outage.

The Root Cause Analysis identifies the root cause of failure and corrective action to prevent a like failure in the future.

9.5 Service Level Agreement

The NGA 911 IMS Policy Rules will be pre-defined and documents included all SLA measurements. If an outage/trouble is reported that triggers an SLA the system automatically sends an alarm to the Executive Management team and a Trouble Ticket is created in the IMS. The IMS automatically keeps a Trouble Ticket Log that will include:

- The date and time the failure was reported or the system alarm of failure
- Each PSAP affected by the failure
- The current status of the restoration process
- Tracks the progress and status of restoration
- Date and time the failure is remedied

The IMS is available via a web-portal 24x7x365 and is accessible by the Commission and PSAPs to track the progress of the restorations of failures and to validate SLA calculations.

Service Level Agreement measurements are listed in the Service Level Agreement (SLA) Plan.

10 Risks and Project Milestones

Risk Assessment

To ensure the health of the project, NGA 911 will develop a Risk Assessment Matrix with the Commission. This will allow NGA 911 and the Commission to identify the areas of the project that are most at risk and develop strategies to mitigate these risks.

Risk Assessment Matrix

Risk	Description	Likelihood	Impact	Mitigation

Network	Risk of Network Failures	Very Low	If network is 100% lost to PSAP – Calls will be rerouted	Rerouting Calls to failover PSAP
Delivery	SMS Texting is a connectionless service	Often	Text Communication is not reliable	Since SMS Texting has no receipt mechanism there is never certainty that a message is received. Best practices include resending Texts if expected responses are not received
Legacy OSP	Risk of improper routing due to conflicts in the LDB	Low	Calls will be routed to a State or Regional default PSAP when there are routing issues	Will work with OSPs to minimize the likelihood of routing conflicts
Routing Errors	Risk of receiving corrupted location data (i3)	Very Low	Calls will be routed to a State or Regional default PSAP when there are routing issues	NGA 911 will work to incorporate as many location services as available and based on confidence levels use as alternates for routing
Interoperability	Nonstandard implementations	Very Low	May cause any number of issues	Adhere to fall back scenarios to ensure service even in the event of partial compliance

Project Milestones

NGA 911 will show key events and movement on the project plan using the Project Milestone Report, see Appendix 2.

Project milestones will include but not limited to:

- Identify Key Staff
- PSAP Site Survey Schedule
- NGCS Network Requirements and Final Design Solution
- Acceptance Test Plan
- Training Plan
- Monthly Billing and SLA Plan
- PSAP Cutover Day Plan
- Interface and Integration Plan
- Selective Router Decommissioning Plan
- Delivery of Certificate of System Readiness
- System Acceptance Testing
- Maintenance Plan

11 Change Management Process

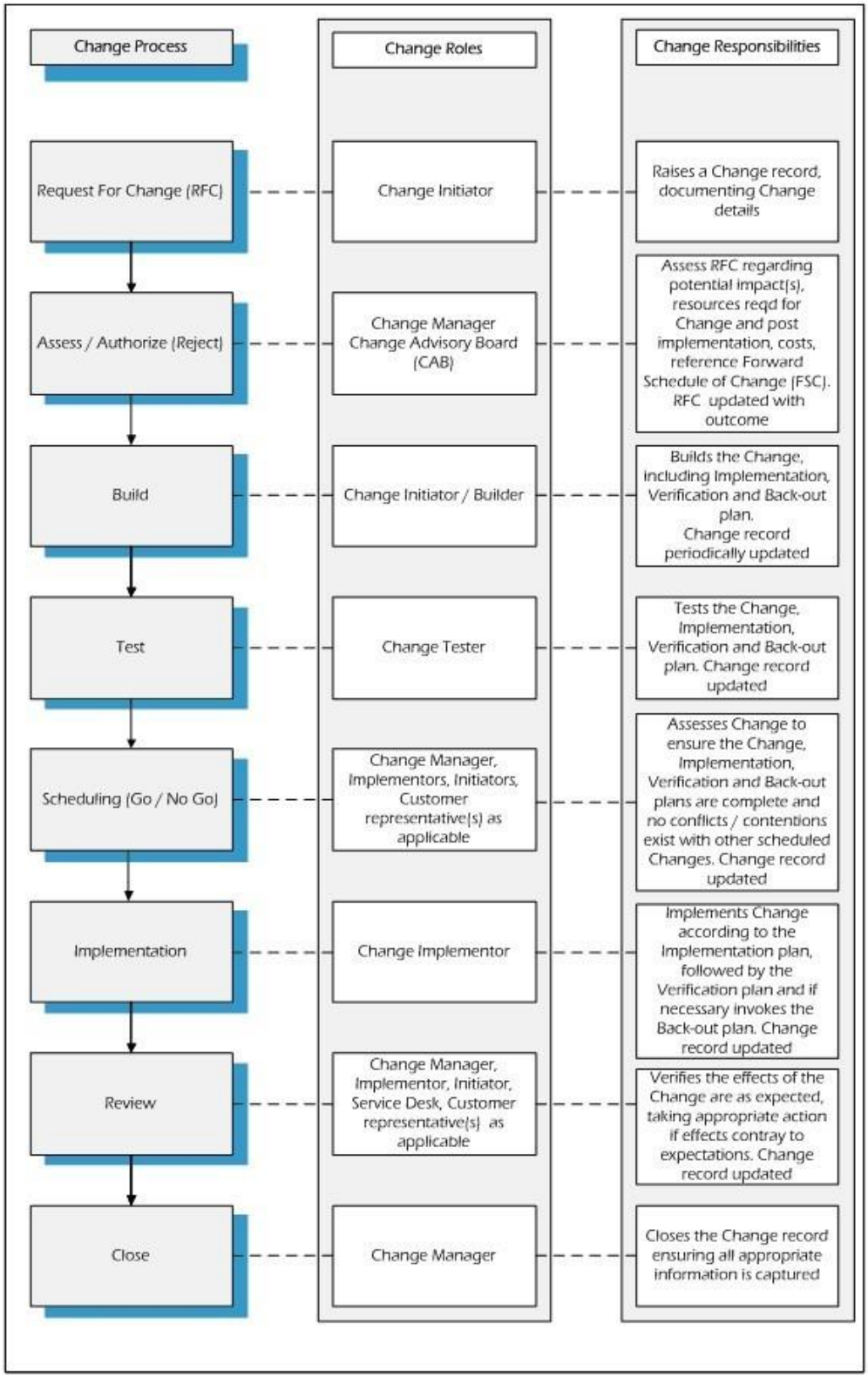
NGA 911 will collaborate with the Commission's Project Manager/Sponsor to develop a Change Management Plan process. The Change Management Plan will establish a Change Management Board that will evaluate and approve all change to scope of the project. The Change Management Plan process will require the following steps:

1) Demonstrate the need/reason for the change
2) Define the type and scope of the change
3) List all stakeholder support and opposition
4) Address roadblocks
5) Present to Change Management Board
6) Track change (Change request form, change log, decisions)

NGA 911 adheres to the eight quality management principles: customer focus, leadership, employee involvement, process approach, system approach to management, continual improvement, factual approach to decision making and mutually beneficial supplier relationships.

Continual improvement processes will be integrated throughout the program, from commencement to ongoing operations, to assure compliance with requirements, fulfilment of contract performance standards and the delivery of increasing customer satisfaction.

Please see the NGA 911 Change Management Workflow:



Appendix 1: Cutover Plan

1. Index

0	Document Control
1	Cutover
2	Cutover Escalation
3	Post Implementation Support
4	On Site Resource
5	War Room/Conf Bridge
6	Risk Score Card
7	Contingency/Roll Back Plan

2. Document Control

Change Record

Date	Author	Change Reference

Owner

Name	Position

Contributors

Name	Position

Reviewers

Name	Position

Issue List

Ref No	Issue Description	Date Reported	Status	Resolution Description	Date Resolved	Resolution Accepted By

3. Cutover Plan

Activity	Time Required	Questions/Comments	Start	End
Preparation Activities				
Map system activities				
Preliminary Activities				
Cutover Checkpoint Meeting 1				
Task 1				
Task 2				
Task 3				
Decision to Move Forward				
Post-Production Follow Up Meeting				
Test to confirm working without issues				
Monitor				
Rollback Required				
Restore to Pre-Cutover Condition				

4. Cutover Escalation

Support Escalation List

Level 0 - War Room - On Site

Level 1 - Helpdesk

Name	Office Number	Mobile Number	Email
Helpdesk	(877) 899-8337 x 2	NA	Services@NGA911.com

Level 2 - Network Operations Manager

Name	Office Number	Mobile Number	Title	Email
Provided Upon Award				

Level 3 - Executive Management

Name	Office Number	Mobile Number	Title	Email
Provided Upon Award				

Level 4 - Chief Executive Officer

Name	Office Number	Mobile Number	Title	Email
Provided Upon Award				

5. Post Implementation Support

Version History	Version No	Author	Date	Status: Draft/Approved

Achievement of Expected Deliverable/Task	Details of Expected Achievement	Details of Issues Reported	End User Feedback	Actions Recommended

6. Onsite Resource

OnSite Manager:

Name	Office Number	Mobile Number	On Site Shift	Email
Provided Upon Award				

OnSite Team:

Name	Office Number	Mobile Number	On Site Shift	Email
Provided Upon Award				

7. War Room

Location		
Conference Bridge		

OnSite Manager:

Name	Office Number	Mobile Number	On Site Shift	Email
Provided Upon Award				

OnSite Team:

Name	Office Number	Mobile Number	On Site Shift	Email
Provided Upon Award				

8. Risk Scorecard

Criteria	1 No Impact	2 Low Impact	3 Medium Impact	4 High Impact	5 Show Stopper
Site					
Technology					
Training					
Data Migration					
Sustainment					
Functionality					
Cutover Planning					
Overall Risk Score:					

9. Rollback Plan

Authority for Back-Out	Title

Activity	Time Required	Questions/Comments	Start	End
Back-Out Procedure				
Back-Out Verification Procedure				
Rollback Procedure				
-				
Rollback Considerations				
Rollback Criteria				
Rollback Risks				
-				
Rollback Verification Procedure				

Appendix 2: Project Milestones Template

Project Milestone Report #8	
Project Name:	**Prepared Date:**
Contract number:	**%Complete: 100%**
Project Start Date:	**Project End Date:**
Milestone Name: Final Systems Acceptance	**Milestone Due Date:**
Milestone Description:	
PSAP Project Manager:	**NGA 911 Project Manager:**
Signature:	**Signature:**
Agreement to Adjust Milestone Due Date	
Approved by xxx:	Approved by NGA 911:
PSAP Project Manager:	**NGA 911 Project Manager:**
Signature:	**Signature:**
Reason for Adjusted Milestone Due Date:	
Project Milestone Status	
Project Milestone Status (Circle One)	On Time/Within Scope At Risk In Danger
Project Milestone Status/Risk Details:	

Appendix 3: NG9-1-1 Functions and Services Acceptance and Authorization Template

This document is a template that will serve as a starting point to develop a checklist that shall serve as notice from the Commission to NGA 911 that the NG Functions and Services are acceptable, as stated below and the Contractor may invoice the Commission.

All Information to be completed by the Contractor only

	Commission Initial
❑ NG Text to 9-1-1 – Web Based OTT	_____
❑ NG Text to 9-1-1 – Integrated	_____
❑ Legacy PSAP Gateway	_____
❑ Independent Verification & Validation	_____
❑ Regional Interoperability Connection	_____
❑ PSAP Integration	_____
❑ Performance Reporting	_____
❑ Call Logging	_____
❑ Statewide Outage Reporting	_____
❑ NRC Project Initiation and Design	_____
❑ Statewide 911 GIS	_____
❑ Selective Routing – as a standalone service	_____
❑ GIS Data synchronization	_____
❑ Alert and Warning System	_____

Minor Discrepancies:

_____

_____

As the authorized representative of:

_____ *(Commission NG9-1-1 Manager),*

I hereby acknowledge receipt, installation and satisfactory performance of the service. If minor discrepancies exist, but do not keep the service from performing in accordance with the contracted terms and conditions, these discrepancies are noted above.

AUTHORIZED BY:

_____ _____

Signature Date

_____ _____

Printed/Typed Name Title

Appendix 4: Certificate of System Readiness Template

The Certificate of System Readiness Template is in Word format.

NGA 911 NETWORK SERVICE PROVIDER	PSAP NAME	TODAY'S DATE:

Start Date of System Acceptance:	End Date of System Acceptance:
PSAP Representative Name:	PSAP Representative Signature:
Commission Representative Name:	Commission Representative Signature:

All of the above signed Representatives hereby acknowledge receipt, installation and satisfactory performance of the Next Generation 9-1-1 Services. This Certificate of System Readiness confirms the NG9-1-1 Services have successfully completed the 45 calendar days Acceptance Test Plan (ATP). Any discrepancies noted during the ATP shall be noted on the Final Test Report.

PSAP, Nebraska

Training Plan

June 2020

Draft

Document History

Index	Date	Author(s)	Description	Version
1	9/1/2019	S. Guenther	Draft Version	-a
2	9/30/2019	M. Bland		-b

Table of Contents

1. Introduction 5
1.1 Knowledge Transfer and Training Overview 6
2. Training Sessions 7
2.1 PSAP Training Plan 7
2.1.1 PSAP Train-the-Trainer 7
2.1.1.1 PSAP Training Outline 8
2.2 PSAP Training Plan 8
2.2.1 Admin Training 9
2.2.1.1 Admin Training Outline 9
2.2.2 Train the Trainer Training 9
2.2.2.1 Train the Trainer Training Outline 10
2.2.3 Director/Supervisor Training 10
2.2.3.1 Director/Supervisor Training Outline 10
2.2.4 End User Training 11
2.2.4.1 End User Training Outline 11
2.2.5 GIS User Training 11
2.2.5.1 GIS User Training Outline 12
3. Web-based Portal 12
3.1 Logging on to the NGA 911 Nebraska Web Portal 12
3.2 How to Change your password 13
3.3 How to set your notification settings 16
4. Dashboards 18
5. Help Desk 18
5.1 Create a Help Desk ticket 19
6. Reports 19
6.1 Canned Reports 19
6.2 Ad-Hoc Reports 21
7. Network Monitoring 21
7.1 Network Monitoring Reports 21
8. NOC/SOC 22
8.1 Network Operations Center (NOC) 22

8.2 NOC Responsibilities 22
8.3 NOC Requirements 25
8.4 Security Operations Center (SOC) 26
9. Problem Management 27
9.1 Change Control Service Request Process 27
9.2 Change Control Process 29
10. GIS 30
10.1 GIS Process 30
11. Online Resources 41
12. Disaster Recovery (DR) 41
12.1 Service Restoration 42
12.1 Iterative, Continuous Assessment DevOps Process 42
12.1 Outage Mitigation 43
13. NIMS 43
a. Web-based Portal 44
13.1 Recovery Processes 45
13.2 Communications Response Team 46
2.1.4 Employee Training Exercises 48
2.1.5 Disaster Recovery (DR) Leadership Training 49
2.1.6 Employee Contact Lists 49
14. System and Service Availability 50
14.1 Network Monitoring 50
14.2 Alarming 50
14.3 Maintenance 51

1. Introduction

This NGA 911 Training Plan (RTP) for PSAP will be the guideline for the training NGA 911 will provide for PSAP personnel, PSAP Admins, Trainers, GIS personnel, and each PSAP end-user prior to scheduled "Go Live" date. We have stylized training sessions for the PSAP personnel, PSAP Admins, Trainers, GIS personnel, and the PSAP end-user.

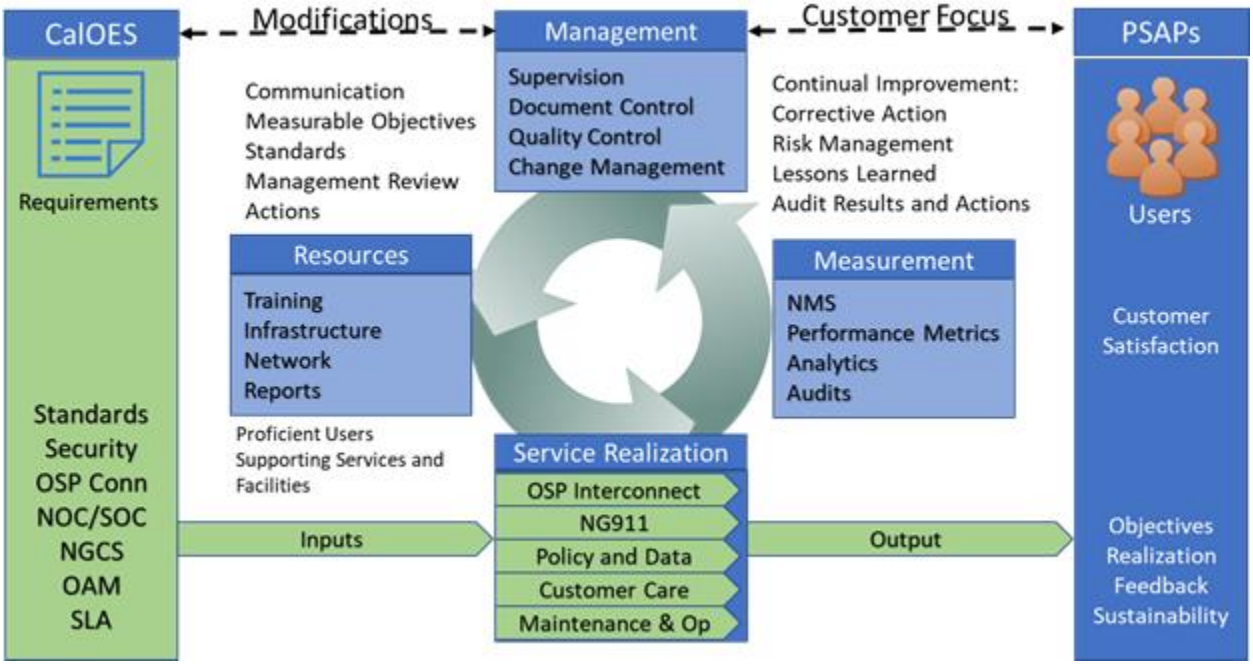
The focal point of our processes is Service Realization in the form of training to the highest possible standards; and continual improvement of services and capabilities for the direct benefit and to the satisfaction of the customer - the first responder community. Key elements to achieving these goals are, amongst others:

(1) meeting State and County objectives

(2) a responsive and effective customer care focused approach

(3) consistent maintenance and operations to include continual enhancement of features and capabilities

(4) a sustainable business model for the State



1.1 Knowledge Transfer and Training Overview

NGA 911 is a customer-oriented organization that takes a systematic approach to Training. Our courses take into account the four (4) perceptual modalities (preferred learning styles): Visual, Aural, Read/Write, and Kinesthetic. NGA 911 has engineered courses that will engage the adult learner on as many of these styles as possible during each course.

To ensure maximum retention of the adult learner we have incorporated the following teaching tools:

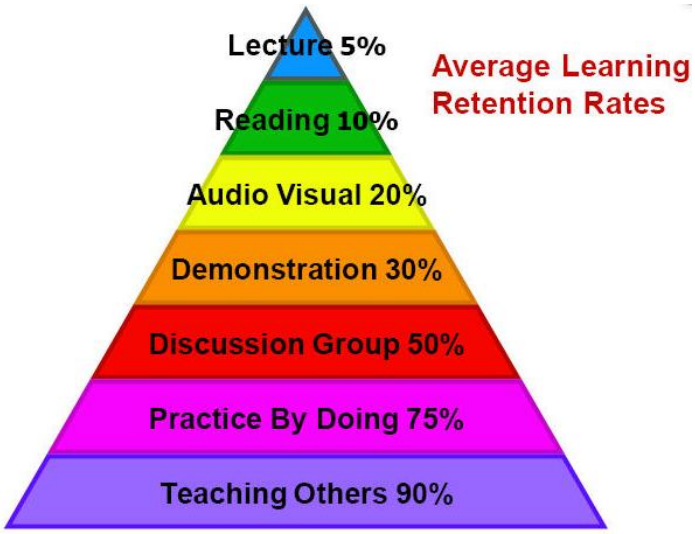
Visual Learners – we provide charts, graphics, and pictures making the training highly visual with screen shots to show the relationships between the tools and the material.

Auditory Learners – we provide the training verbally as they preferred to hear rather than reading or seeing the material displayed visually.

Reading/Writing Learners – we provide annotated handouts of the presentation so they can read along and provide the chance to write down what they have learned.

Kinesthetic Learners – we provide hands-on experience with our training mode of the Web-based portal to practice what they are learning.

By incorporating these teaching tools, we know that the adult learner's retention rate is increased to 75%.



2. Training Sessions

2.1 PSAP Training Plan

50 calendar days prior to the 1st scheduled "Go Live" date in the PSAP will provide NGA 911 the following information for each personnel to have credentials in the Web-based portal:

- First name
- Last name
- Email address
- Mobile phone number
- Role
    - PSAP Personnel
    - Admin
    - GIS
    - End user
- Permissions for jurisdiction associated with

PSAP personnel may have permissions to retrieve analytics and reports from all jurisdictions they have permissions identified.

2.1.1 PSAP Train-the-Trainer

NGA 911 will provide a Train-the-Trainer session not to exceed one (1) eight (8)-hour training for designated PSAP personnel within 45 calendar days of the 1st scheduled "Go Live" date in the PSAP. NGA 911 will provide all training resources at the time of training. NGA 911 will maintain current versions of all training materials on our Web-based portal that can be accessed 24x7x365.

NGA 911 will host training sessions at a location decided by PSAP. The training will accommodate as many PSAP personnel as required and per the meeting room capacity.

2.1.1.1 PSAP Training Outline

Attendees are encouraged to ask questions during the sessions for maximum retention. Train-the-Trainer session will include hands on training for:

- Web-based portal
- Dashboards
- Help Desk Ticketing
- Trouble Reporting Escalation
- Reports
    - Canned
    - Ad-hoc
- Network Monitoring
- NOC/SOC
- Problem Management
- High level GIS data entry
- Online Resources
    - Training Manuals
    - Training Videos
- Disaster Recovery
- NIMS
- Review
- Questions and Answer

2.2 PSAP Training Plan

50 calendar days prior to the "Go Live" date the PSAP contact person will provide NGA 911 the following information for each personnel to have credentials in the Web-based portal:

- First name
- Last name
- Email address
- Mobile phone number
- Role
    - Director/Supervisor
    - Admin
    - GIS
    - End user
- Permissions for jurisdiction associated with

The credentialed personnel may have permissions to retrieve analytics and reports from their jurisdiction depending on their role.

NGA 911 will host training sessions at a location agreed upon by the PSAP and NGA 911. The training will accommodate as many PSAP personnel as required and per the meeting room capacity.

2.2.1 Admin Training

NGA 911 will provide the Admin Training session not to exceed one (1) eight (8)-hour training for designated PSAP Admin. The Admin session will be held within 45 calendar days of the scheduled "Go Live" date for the PSAP. NGA 911 will provide all training resources at the time of training. NGA 911 will maintain current versions of all training materials on our Web-based portal that can be accessed 24x7x365.

NGA 911 will host training sessions at a location agreed upon by the PSAP and NGA 911. The training will accommodate as many PSAP personnel as required and per the meeting room capacity.

2.2.1.1 Admin Training Outline

Attendees are encouraged to ask questions during the sessions for maximum retention. Admin session will include hands on training for:

- Web-based portal
- Requesting personnel credentials
- Dashboards
- Help Desk Ticketing
- Trouble Reporting Escalation
- Reports
    - Canned
    - Ad-hoc
- Network Monitoring
- NOC/SOC
- Problem Management
- High level GIS data entry
- Online Resources
    - Training Manuals
    - Training Videos
- Disaster Recovery
- NIMS
- Review
- Questions and Answer

2.2.2 Train the Trainer Training

NGA 911 will provide the Train-the-Trainer Training session not to exceed one (1) eight (8)-hour training for designated Admin the Admin session within 45 calendar days of the scheduled "Go Live" date for their PSAP. NGA 911 will provide all training resources at the time of training. NGA 911 will maintain current versions of all training materials on our Web-based portal that can be accessed 24x7x365.

NGA 911 will host training sessions at a location agreed upon by the PSAP and NGA 911. The training will accommodate as many PSAP personnel as required and per the meeting room capacity.

2.2.2.1 Train the Trainer Training Outline

Attendees are encouraged to ask questions during the sessions for maximum retention. Train-the-Trainer session will include hands on training for:

- Web-based portal
- Dashboards
- Help Desk Ticketing
- Trouble Reporting Escalation
- Reports
    - Canned
    - Ad-hoc
- Network Monitoring
- NOC/SOC
- Problem Management
- High level GIS data entry
- Online Resources
    - Training Manuals
    - Training Videos
- Disaster Recovery
- NIMS
- Review
- Questions and Answer

2.2.3 Director/Supervisor Training

NGA 911 will provide the Director/Supervisor Training session not to exceed one (1) eight (8)-hour training for designated Directors/Supervisors. The Director/Supervisor session within 15 calendar days of the scheduled "Go Live" date for their PSAP in the PSAP Region. NGA 911 will provide all training resources at the time of training. NGA 911 will maintain current versions of all training materials on our Web-based portal that can be accessed 24x7x365.

NGA 911 will host training sessions at a location agreed upon by the PSAP and NGA 911. The training will accommodate as many PSAP personnel as required and per the meeting room capacity.

2.2.3.1 Director/Supervisor Training Outline

Attendees are encouraged to ask questions during the sessions for maximum retention. Train-the-Trainer session will include hands on training for:

- Web-based portal
- Dashboards
- Help Desk Ticketing
- Trouble Reporting Escalation
- Reports
    - Canned
    - Ad-hoc
- Network Monitoring

- NOC/SOC
- Problem Management
- High level GIS data entry
- Online Resources
    - Training Manuals
    - Training Videos
- Disaster Recovery
- NIMS
- Review
- Questions and Answer

2.2.4 End User Training

NGA 911 will provide the End User Training session not to exceed one (1) eight (8)-hour training for designated Admin the Admin session within 15 calendar days of the scheduled "Go Live" date for their PSAP. NGA 911 will provide all training resources at the time of training. NGA 911 will maintain current versions of all training materials on our Web-based portal that can be accessed 24x7x365.

NGA 911 will host training sessions at a location agreed upon by the PSAP and NGA 911. The training will accommodate as many PSAP personnel as required and per the meeting room capacity.

2.2.4.1 End User Training Outline

Attendees are encouraged to ask questions during the sessions for maximum retention. End User session will include hands on training for:

- Web-based portal
- Dashboards
- Help Desk Ticketing
- Trouble Reporting Escalation
- Network Monitoring
- NOC/SOC
- High level GIS data entry
- Online Resources
    - Training Manuals
    - Training Videos
- Disaster Recovery
- NIMS
- Review
- Questions and Answer

2.2.5 GIS User Training

NGA 911 will provide the GIS User Training session not to exceed one (1) eight (8)-hour training for designated Admin the Admin session within 45 calendar days of the scheduled "Go Live" date for their

PSAP in the PSAP Region. NGA 911 will provide all training resources at the time of training. NGA 911 will maintain current versions of all training materials on our Web-based portal that can be accessed 24x7x365.

NGA 911 will host training sessions at a location agreed upon by the PSAP and NGA 911. The training will accommodate as many PSAP personnel as required and per the meeting room capacity.

2.2.5.1 GIS User Training Outline

Attendees are encouraged to ask questions during the sessions for maximum retention. End User session will include hands on training for:

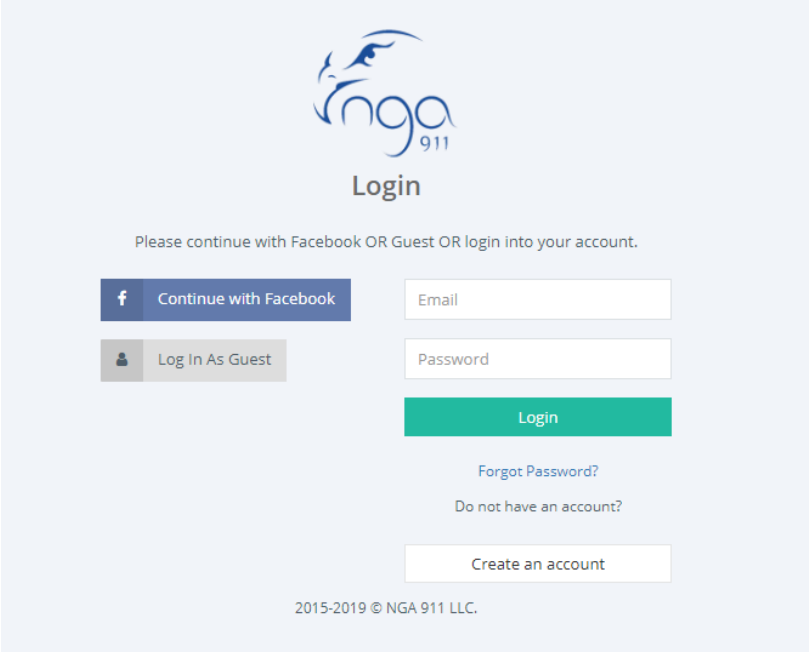
- Web-based portal
- Dashboards
- Help Desk Ticketing
- Trouble Reporting Escalation
- Detailed GIS data entry
- Online Resources
    - Training Manuals
    - Training Videos
- Review
- Questions and Answer

3. Web-based Portal

3.1 Logging on to the NGA 911 Nebraska Web Portal

To access the secure portal, you will be required to log into the system by following the outlined steps:

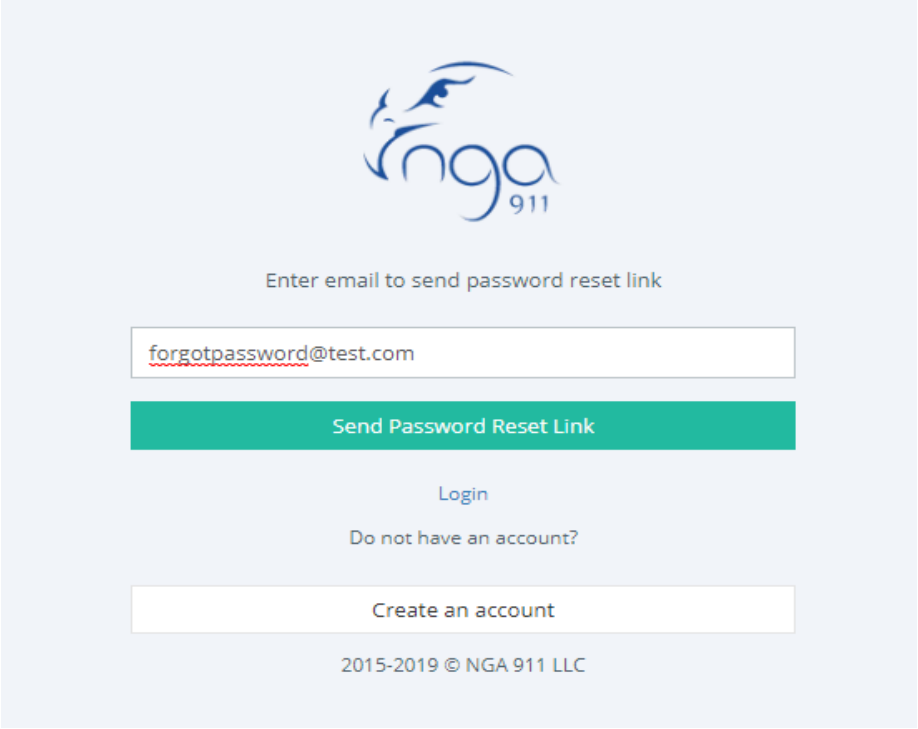
1. Launch your browser (Chrome, Internet Explorer, Microsoft Edge, Firefox) and enter the following URL into the address bar of your browser: https://psap.ca.nga911.com/auth/login
2. On the NGA 911 Nebraska login page, enter your credentials to login.



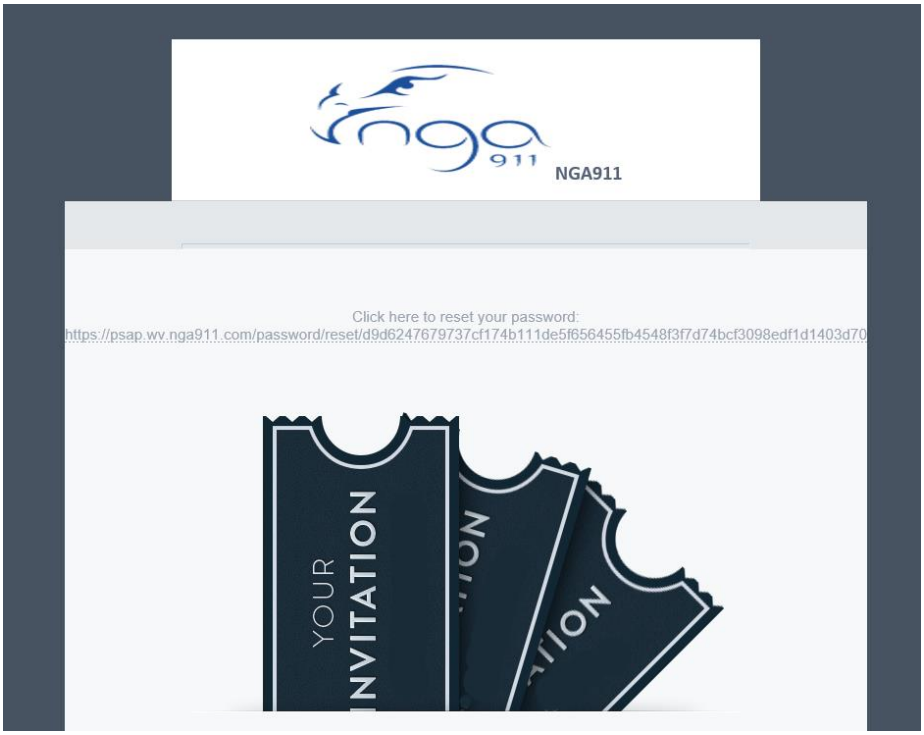
3. In the Email box, enter the email that has been provided to NGA 911 by your Administrator.
4. In the Password box, enter your password (The NGA 911 default password is Password123).
5. Click Login.
6. Once you have clicked Login you will be redirected to the Dashboard page.

3.2 How to Change your password

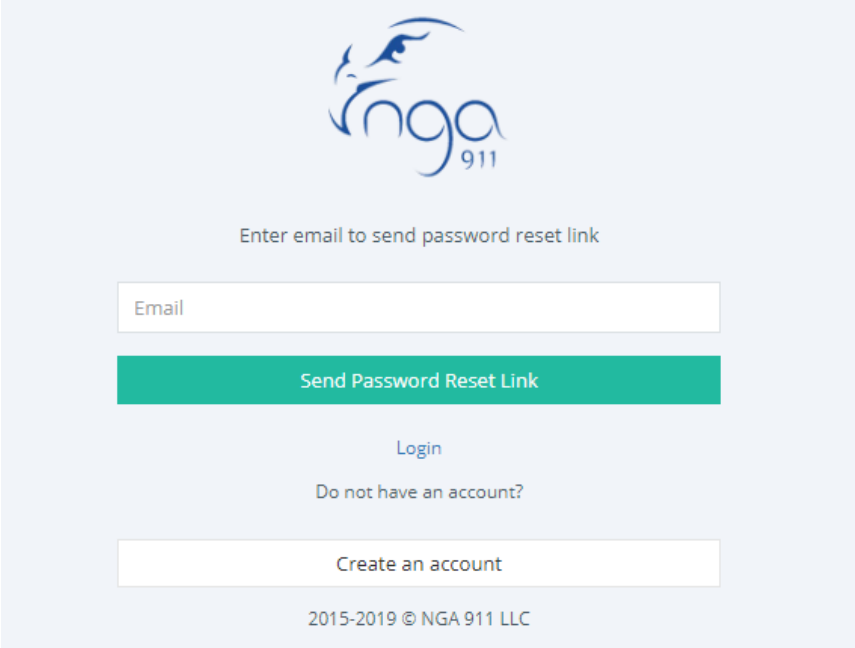
1. Launch your browser (Chrome, Internet Explorer, Microsoft Edge, Firefox) and enter the following URL into the address bar of your browser: https://psap.ca.nga911.com/auth/login
2. Click on the Forgot Password link.
3. In the Email box, enter the email address that was provided to NGA 911.



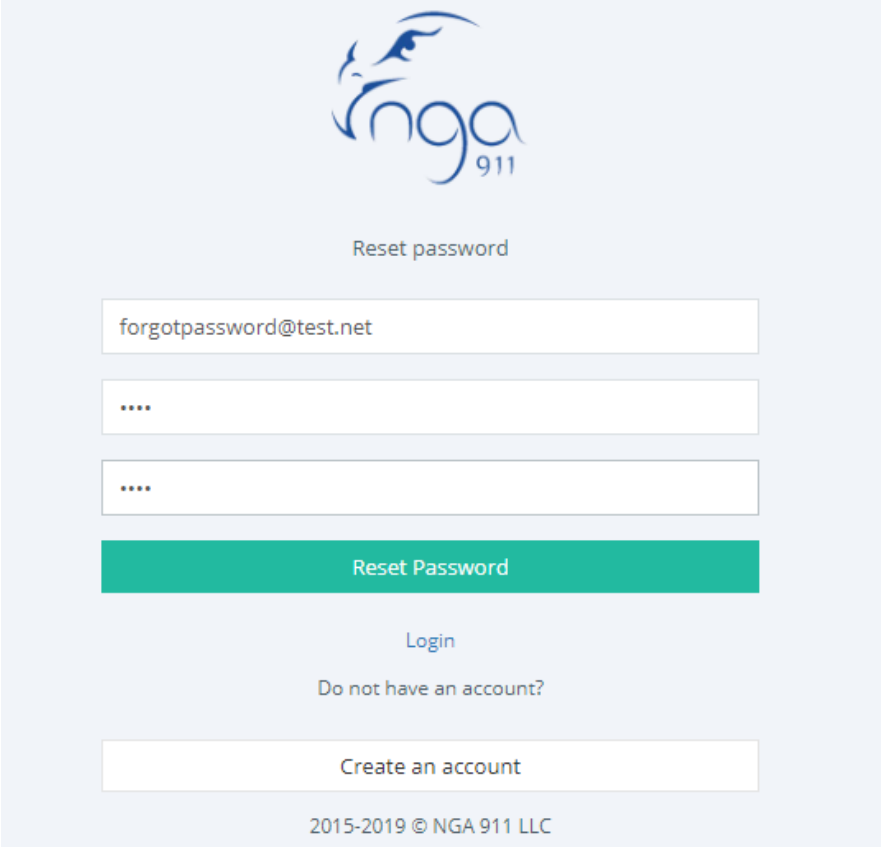
4. Click Send Password Reset Link.
5. Once you have clicked Send Password Reset Link you will receive an email to reset your password.
6. Once you receive the email to reset your password click on the link provided in the email.



7. Click on the link from the email received and you will be taken to the Reset Password web page.



8. In the Email box, enter the email address that was provided to NGA 911.



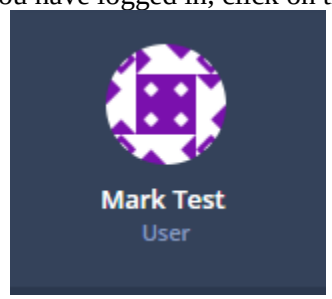
9. In the Password box, enter your new password.

10. In the Confirm Password box, re-enter your new password.
11. Click Reset Password.

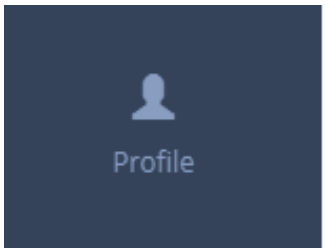
12. You will now be redirected to your NGA 911 Dashboard page.

3.3 How to set your notification settings

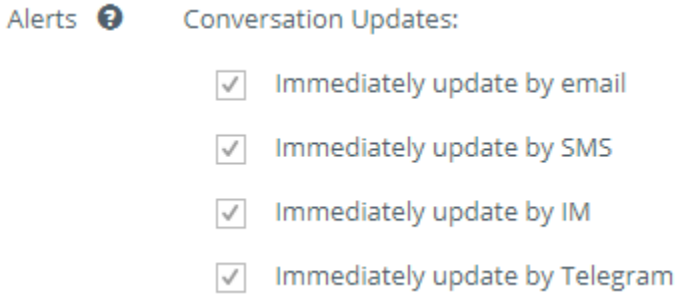
1. Launch your browser (Chrome, Internet Explorer, Microsoft Edge, Firefox) and enter the following URL into the address bar of your browser:
   https://psap.ca.nga911.com/auth/login
2. Once you have logged in, click on the User Icon located in the upper left hand corner



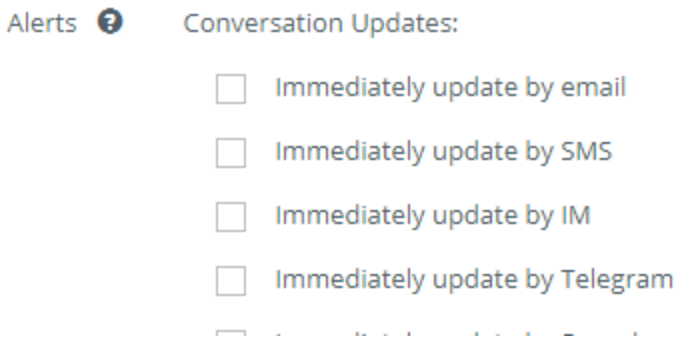
3. Or click on the Profile icon.



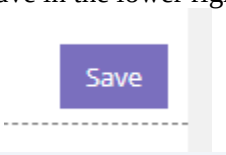
4. Once you have clicked on the User Icon or Profile icon you will be directed to your Personal Profile page.
5. Locate the Alerts field.
6. Under the Alerts field you can select the method in which you wished to notified of any Conversation updates.
7. Verify that each method of contact that you would like to utilize contains a check mark.

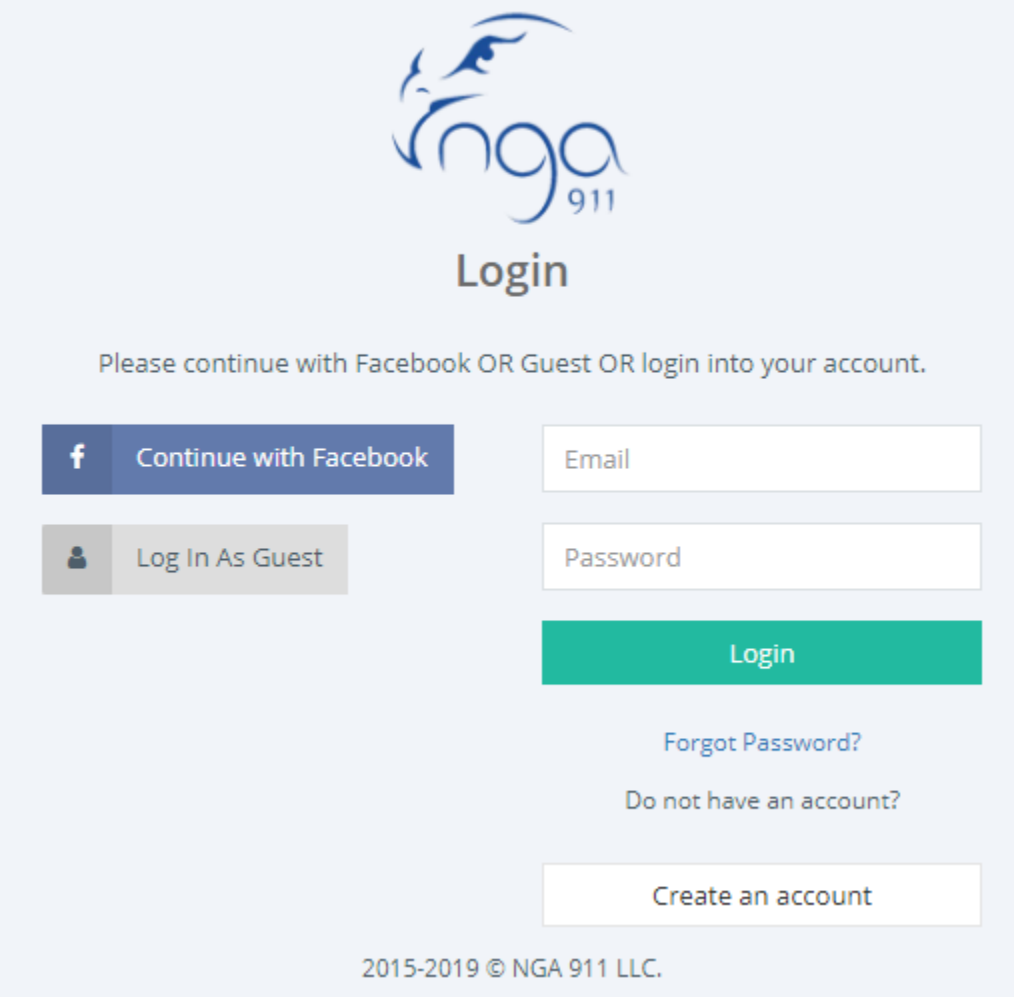


8. Verify that each method of contact you would not like to utilize does not contains a check mark.



9. Click Save in the lower right-hand corner.

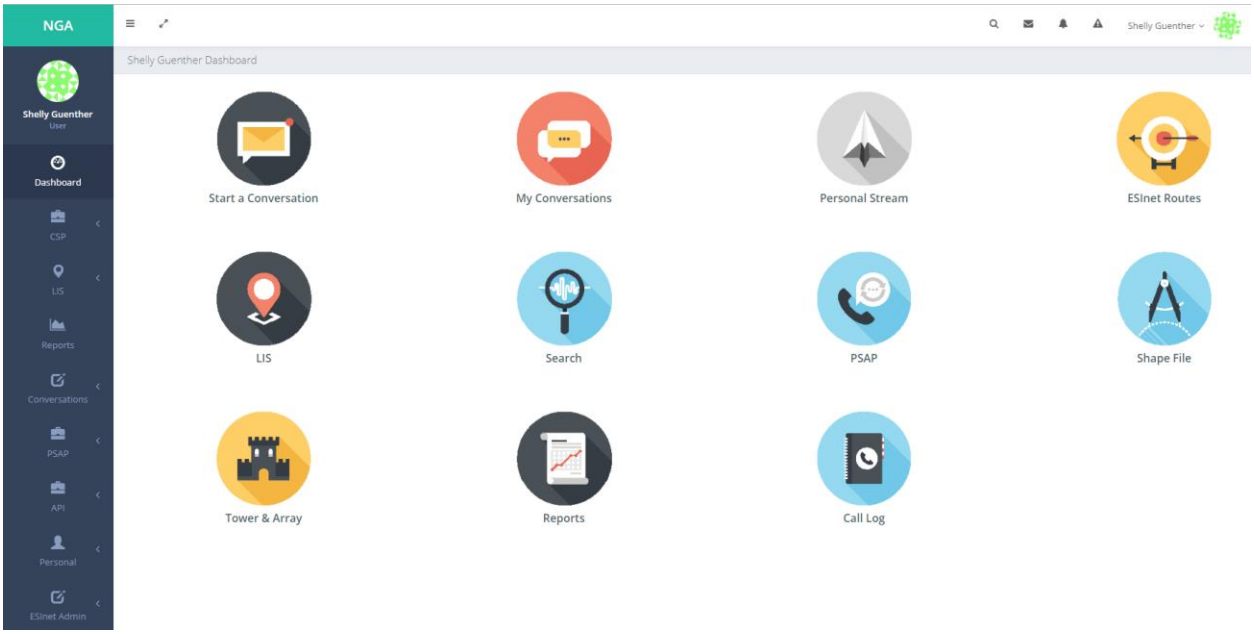




Upon successful log on you will see the Dashboard.

4. Dashboards

The NGA 911 Dashboards will only display the features you have permissions granted. You may not see all of the below icons.



5. Help Desk

The NGA 911 Help Desk is on the Web-based portal.

The credentialed personnel will log into the NGA 911 Web-based portal at: https://csp.nga911.com/dashboard

You will be required to log into the system.

After logging on you will select the Help Desk icon:

You will then be able to:

- Create a Help Desk ticket
- View your Help Desk tickets
  - Active
  - Closed
- Add notes to an open ticket
- Escalate an open ticket

5.1 Create a Help Desk ticket

1. Create a ticket in www.csp.nga911.com
2. Add the affected users information;
    1. In the title of the conversation add a tag before the description. (Example; [Bug], [Feature], [Urgent], [Android], [IP PBX] or [Telnyx].)
    2. URL (Example; www.csp.nga911.com, www.psap.ca.nga911.com, www.l.communitywatch.io)
    3. User Name (Example; marklemonn@nga911.com)
    4. Description of the problem (Example; When logging into www.csp.nga911.com the user (marklemonn@nga911.com) is experiencing an invald credential error)
    5. Screenshot of the issue and/or a Selenium IDE exported file. (if you are providing a Selenium file please record the issue then save the file.)
3. Add screenshots and Selenium file.
4. Assign the ticket to the R&D community. (Do not add users to the ticket as collaborators. Only assign the ticket to the R&D community)
5. Set the status of the ticket to "Queue".

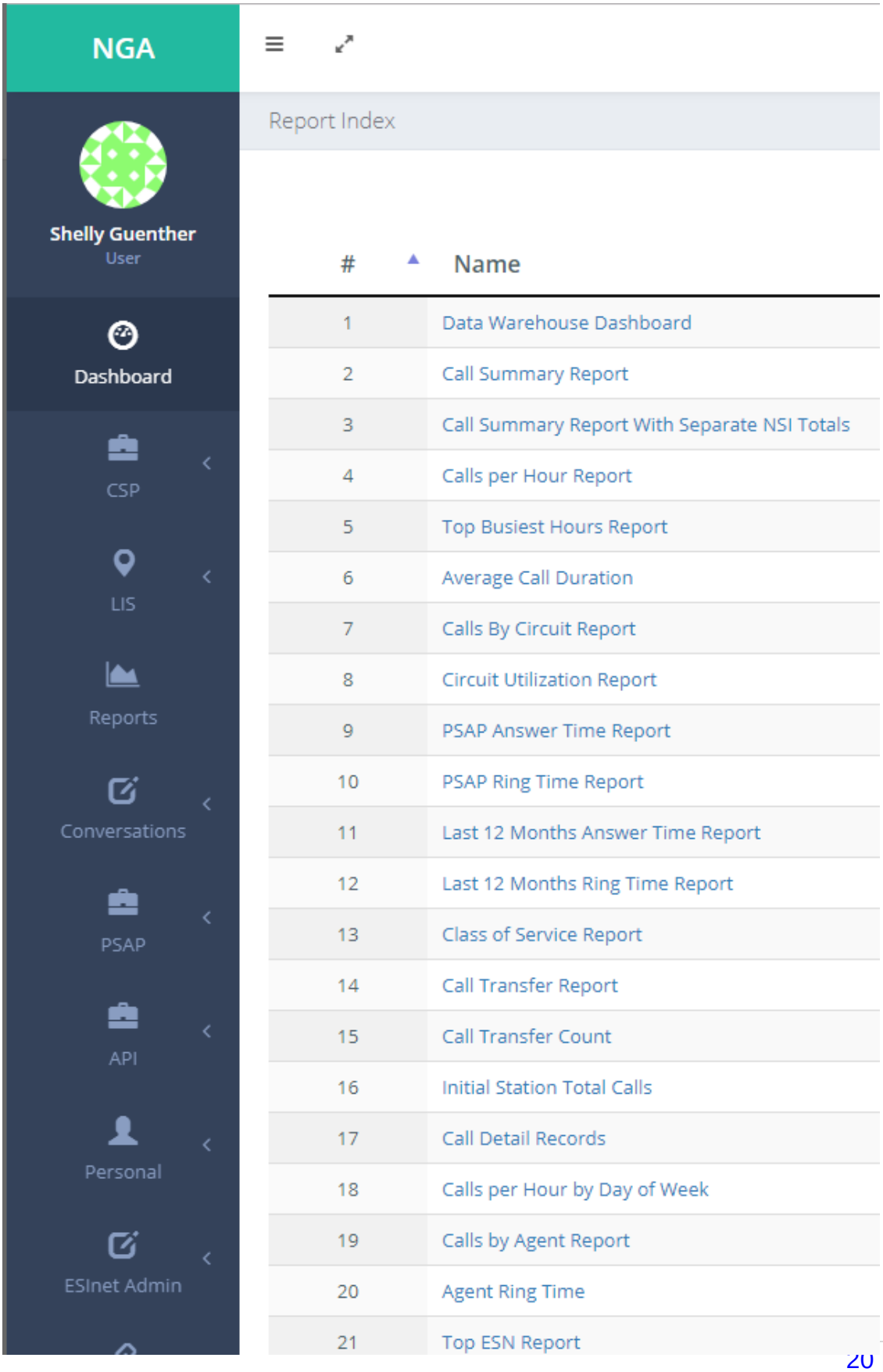
6. Reports

The NGA 911 has a Reporting function on the Web-based portal.

Reports

6.1 Canned Reports

1. Create a report in www.csp.nga911.com
2. Select the report to be created;
    1. In the drop-down menu select the report title. (Example; [Network performance], [IP usage and allocation], [Root cause analysis], [Calls by date], [Total call duration] or [Call transfers].)
    2. Time frame for the report (Example; From 01/01/2020; To 01/31/2020)
    3. In the drop-down menu select the call taker positions for the report. (Example; [Call taker station 1], [All call taker stations].)
    4. Click on all the stations required.
3. Select report delivery manner (Example; [Email], or [Print].)



#	Name
1	Data Warehouse Dashboard
2	Call Summary Report
3	Call Summary Report With Separate NSI Totals
4	Calls per Hour Report
5	Top Busiest Hours Report
6	Average Call Duration
7	Calls By Circuit Report
8	Circuit Utilization Report
9	PSAP Answer Time Report
10	PSAP Ring Time Report
11	Last 12 Months Answer Time Report
12	Last 12 Months Ring Time Report
13	Class of Service Report
14	Call Transfer Report
15	Call Transfer Count
16	Initial Station Total Calls
17	Call Detail Records
18	Calls per Hour by Day of Week
19	Calls by Agent Report
20	Agent Ring Time
21	Top ESN Report

6.2 Ad-Hoc Reports

This section will be configured after collaboration with PSAP.

7. Network Monitoring

The NGA 911 continuously monitors the network. The NOC has an automated system looking at any anomalies along with highly trained humans visually monitoring the network and all alarms.

The credentialed user can create network monitoring reports.

7.1 Network Monitoring Reports

1. Create a report in www.csp.nga911.com
2. Select the report to be created;
    1. In the drop down menu select the report title. (Example; [Network performance], [IP usage and allocation], [Root cause analysis], [Calls by date], [Total call duration] or [Call transfers].)
    2. Time frame for the report (Example; From 01/01/2020; To 01/31/2020)
    3. In the drop down menu select the call taker positions for the report. (Example; [Call taker station 1], [All call taker stations].)
    4. Click on all the stations required.
3. Select report delivery manner (Example; [Email], or [Print].)

8. NOC/SOC

8.1 Network Operations Center (NOC)

The NOC provides a key support role in the DR and its contact information is provided below:

Contact Information Center

Primary Contact:

Phone: 800-873-3822, Option #2

Web Portal: xxxx

E-Mail: xxxx

NOC Escalation Contact Information Table

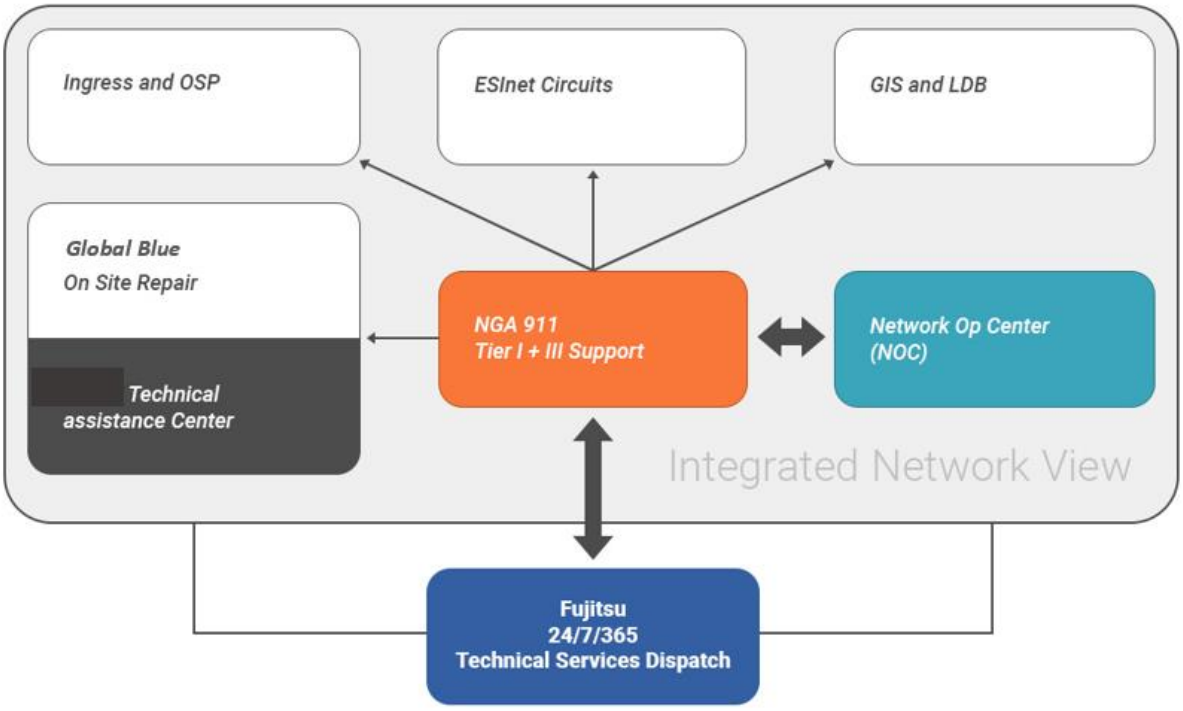
Contact Order	Contact Name	Contact Position	Office Phone (O) Mobile Phone (M)	Email Address
1	Rotational Duty Engineer	Rotational Duty Engineer	800-873-3822 Option 2	xx
2	James Bolden	Shift Lead	xx	xx
2	Dale Price	Shift Lead	xx	xx
3	Brandon Lewis	NOC Manager	xx	xx
4	Tony Kriska	Service Delivery Manager	xx	xx
5	Greg Butler	Director Services Delivery	xx	xx

8.2 NOC Responsibilities

NOC Responsibilities

- NOC will provide premium monitoring services through the Primary Operations Center or through a secondary Operations Center. The managed services provided encompass fault, configuration, performance and network management functions to support the network on a 7x24x365 basis.
- NOC is a Tier 1, Tier 2 and higher NOC monitoring service which will interface with the Service Operations Center, Field Services Teams, and Customer Technical Points of Contact, on the exchange of trouble tickets and network issues.

The diagram below depicts the Interactions between the various field, operational, and support offices in terms of delegation and assignment of Tiered Support for normal and DR operations.



- NOC will report problems, provide updates, and provide resolution status pertaining to the network via email or telephone and E-bond.
    - NOC will initially report trouble to the Priority Response-Live Answer Hotline by calling 1-866-xxx-xxxx (xx@xx.com).
    - NOC will send communication templates in support of trouble efforts.
- NOC will provide on-site technical support for Break/Fix repair of the network through Priority Response. The technician will work with the NOC to coordinate actions and resolution efforts during the technician's time onsite. The technician will go to the site equipped with appropriate test equipment and supplies to

troubleshoot and isolate the issue. Additional parts may be needed and will be coordinated for deployment at time determined to complete the repairs.

- Certain sites will be supported by XX On-Site Technicians and others will be supported by XX On-Site Technicians.
  - All dispatches will be determined by the NOC based on the NGA 911 primary response areas.
  - Primary Network Vendor is determined within the Siebel ticket. On-Site Technical Dispatch Services shall be performed by XX.
- NOC will dispatch Technicians in NGA 911's response areas. NGA 911's contractual SLA is to arrive on-site within 4 hours starting from the time the Technician is dispatched from the NOC.

- NOC will make every effort to schedule potential service affecting actions in a mutually agreed maintenance window depending on the nature and severity of the alarm. In the event of an emergency maintenance window, NOC will provide as much advance notice as possible. In the event NOC is not able to reach DR Management Team within 15 minutes of an emergency maintenance dispatch decision, NOC will take reasonable action to restore the network.
- NOC will provide performance management which entails monitoring, alerting, evaluation, and reporting capabilities for network status and activity. Performance management is provided to the extent of the Device, Software and Element Management System (EMS) capabilities.
- NOC will warehouse and manage spares and contract obligations with the equipment vendor for repairs and return to service.
- NOC will warehouse, deliver, and manage the logistics to provide spare equipment for all contracted equipment that are at NOC's depot location. NOC will ensure that the proper inventory level of spares and depots are established.
- NOC will manage the return of failed equipment sent in for repair with the equipment vendor.
- NOC will work with the fiber vendors through the LOA which has been provided by PSAP. If it is determined that the incident is related to fiber, NOC will interface, pass information, troubleshoot, and escalate as needed with the fiber vendors for all incidents related to fiber.
- NOC is responsible for evaluating the network, including recommending, managing, and coordinating software updates/upgrades on all supported equipment.
- NOC will perform all patch implementations required to resolve a critical, high or medium fault or load major software releases with prior approval.

- Other areas/sites of the Network will be added as the Management-Take-Over (MTO) dates and integration processes are met and devices are physically connected.
- NOC will take extra precaution to ensure that keys, access badges, or other security tools necessary to accomplish access to a site are accounted for and managed in a secure manner. This requirement includes a Photo ID, a second proof of identity, and documented signatures prior to granting or assigning access or ownership.
- NOC will initiate a conference bridge if requested, or multiple efforts are required to resolve or confirm troubles, questions, or issues.

8.3 NOC Requirements

Basic requirements for all NOC tickets:

- Customer Name
- Subscriber Name
- Address Street, City, State
- Circuit ID's
- System type
- Support engineer name
- Date of creation, closure
- Ticket status (Addressed, Restored, Pending, Closed)
- Troubleshooting and general notes entered into the ticket from either party, NOC and CUSTOMER

Basic requirements for all CUSTOMER tickets:

- Affected Customers
- Site Addresses
- TPOC Contact Information
- Device Names (Host Names/TIDs)
- Account Identifier
- Circuit Identifiers
- CUSTOMER Ticket Number
- NOC Ticket Number

- Alarm Types and Details (Alarm/Severities/Timestamps)
- Actions Taken to Resolve Alarm Issues

Incident Resolution/Notification Matrix / Service Level Objectives (SLO)s

NGA 911 currently uses Siebel to log all incident reports per the Severity listings based on TelCordia GR-929 Standards (Critical, Major, Minor).

Severity	Typical Customer Impact	Customer Notification	Customer Communication
Critical	• Complete loss/critical failure of customer impacting service with no available workaround.	Within 15 Minutes	• Within 30 minutes of event initiation • At each escalation point and/or status change • Within 15 minutes of resolution
Major	• Intermittent loss/degraded performance of a customer impacting service	Within 30 Minutes	• Within 1 hour of event initiation • At each escalation point and/or status change • Within 15 minutes of resolution.
Minor	• No immediate customer impact and/or administration requests users.	Within 8 Hours	• None required for non-service affecting questions. • Within 1 hour of event initiation • At each escalation point and/or status change • Within 15 minutes of resolution

8.4 Security Operations Center (SOC)

The heart of Cybersecurity monitoring and response is our SOC which is subdivided into four major areas of focus: vulnerability and security assessments and analysis, threat research, and forensic capabilities. Each of these is broken down to sub focus groups for a comprehensive approach to surveillance, identification, mitigation, and recovery.

In addition to the above-mentioned protections and precautions, the SOC provides alerts and notifications of suspicious events such as: malware activity, ransomware activity, and port and protocol exploitation. When issues arise the SOC provides the State and PSAPs:

· Alert and notification of activity noticed to the designated staff and the affected PSAPs

· Details on the options for isolation of activity to limit impacts and vulnerabilities

· Notifies the State and PSAPs of any limitations that may result through executing the avoidance measures.

9. Problem Management

The goal of problem management is to minimize the adverse impact of incidents and crisis situations that impede on the successful operation of the business. To achieve this goal, problem management assists incident management by managing all crisis situations and significant incidents.

NOC will produce a credible root cause analysis (RCA) for all crisis situations and significant incidents that were investigated and/or repaired within 30 days of the associated problem and monthly summary of outstanding RCAs. RCAs will be completed within CUSTOMER contractual obligations for Priority Response customers. NOC will ensure that comprehensive and accurate details are recorded for all identified problems and provide details to designated CUSTOMER Managers. The report will include the complete documentation of the RCA as well as recommended solutions to prevent or avoid future failures.

9.1 Change Control Service Request Process

Change Control Service Request Process provides a consistent approach to evaluating and implementing any change. The process allows the assessment of the impact, risk, and a resource requirement associated with proposed change control requests and ensures all parties impacted by the change control have been properly notified and proper approvals have been obtained both externally and internally.

- Simple Change (*Standard*)
    - 2 business day's after all specific details are received and verified for the change requested.
    - Simple changes consist of routine operational MAC request. For example, circuit adds, circuit modification, or circuit decommission.
    - Simple changes submitted simultaneously to exceed (30) individual provisioning efforts will be escalated to a complex change and discussed through CAB review to determine if this is a project.
    - A low priority change request will be treated as a standard request that extends the FOC date beyond 3 business days as agreed upon with the customer.
- Complex Change (*Project*)
    - 14 business day's after all specific details are received and verified for the change requested.
    - A Complex Service request that are beyond routine provisioning scope as stated in the OLA.
        - A Service Request that shifts to a project.
        - All request that require tasks that need to extend over x business days.
        - Service Request that involve tasks that involve external teams.
        - Service Request that involve design testing.

Note: Project is defined as:

- A temporary endeavour with a beginning and an end (date)
- Creates a unique product, service, or result

*** *As defined by PMI®*, reference PMBOK ed. 5, released 2013.

- Critical Change *(Emergency)*
    - 8 hours after all specific details are received, verified and approved for the change requested.
    - Customer driven request that are revenue affecting whether positive or negative that require immediate action.
        - All expedited request will require Change Control Request form, and go through the validation process or receive management approval with a written request from the customer.

- All Emergency requests will impact FOC dates of existing scheduled provisioning activities.

The length of the response is counted in business days from the day the Service Request has been accepted and approved by the NOC Change Control Administrator as referenced on page 56 in the SOW.

The cut-off time of receipt of a Service Request is Friday 1:00 PM Eastern. If a request is received prior to the applicable cut-off time on a business day, NOC will consider that day to be the day of the request. However, if the NOC receives a request after the cut-off time, the NOC will consider that the request was made on the next business day.

- **Change Control Service Request Orders are supported Monday 10:00 AM Eastern through Friday 5:00 PM Eastern excluding NOC's observed holidays.**
- **Equipment installs should be scheduled three business days in advance.**
- **The NOC Standard Maintenance Window for internal systems and tools (NMS, EMS, Servers, etc.) is Tuesday 7:00 PM – Wednesday 1:00 AM Eastern.**

9.2 Change Control Process

The following sections outline the guidelines and describe the types of change request(s) and the procedures in which to be followed.

The purpose of the Change Control Request (CCR) procedure is to define what information and responses the PSAP is responsible for providing when requesting network modifications to be performed by the NOC.

The CCR procedure ensures NOC standards are applied to Moves, Adds, Changes and Disconnects (MACD) requested by PSAP.

The process begins when a CCR form is submitted via email to xxxx@fnc.nga911.com. The process consists of five phases, each controlled via workflow gates in Siebel:

Review

The review phase begins with a submitted CCR form from PSAP, which is then validated for correct information. Once all information is verified, the CCR is assigned a ticket number. After a ticket number has been provided, the Service Request Team (SRT) will verify engineering information and promote the ticket to the Build phase.

Build

The build phase begins when the completed review phase promotes the workflow in Siebel (NOC Ticketing System). The SRT will verify capacity, update inventory, and design topology, then send the ticket number to the required team to perform scope of work as described in the ticket.

Ready for Operation (RFO)

The RFO phase begins when all layer one facilities are in place and provisioned for operation. Any changes in provisioning will be recorded and testing (if applicable) will be completed in this stage. Once PSAP accepts testing results, the RFO phase is complete.

Ready for Service (RFS)

The RFS phase contains risk assessment, and the final accept/reject decision. Once accepted, the monitoring devices are turned on.

Management Take Over (MTO)

MTO is the final phase in the procedure and consists of notification to PSAP of MTO status. The circuit is now being monitored and ticketing has been activated. The ticketing system is updated with any notes and closed. This ends the CCR process.

PSAP Notification Process

NGA 911 has Service Level Agreements with PSAP requiring a 5-minute response time for alarm notifications.

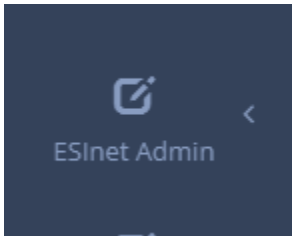
- Notifications will go to the Operations Team email distribution lists:
  - xx@xx.com (TBD)
  - xx@xx.com (TBD)
  - An email forwarder for each Notification Group will send incoming notifications to the appropriate subscriber TPOC(s), and Priority Response.
  - As alarm/condition notifications are sent, the standard operations ticketing process also occurs.
  - PSAP devices have been organized into two Notification Groups. Those managed by NOC and those managed by PSAP.

10. GIS

NGA 911's portal allows the user to upload GIS files.

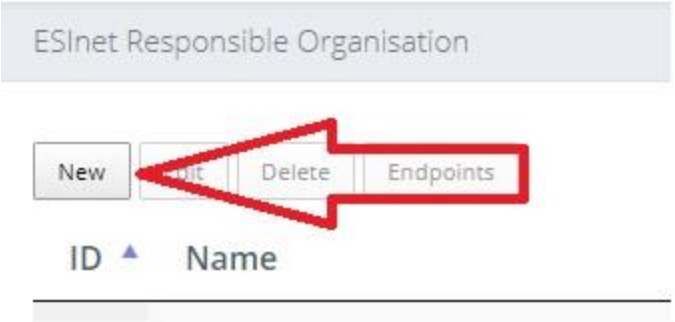
10.1 GIS Process

20. On the left side of the screen scroll until you find the "ESInet Admin" and click on the arrow.

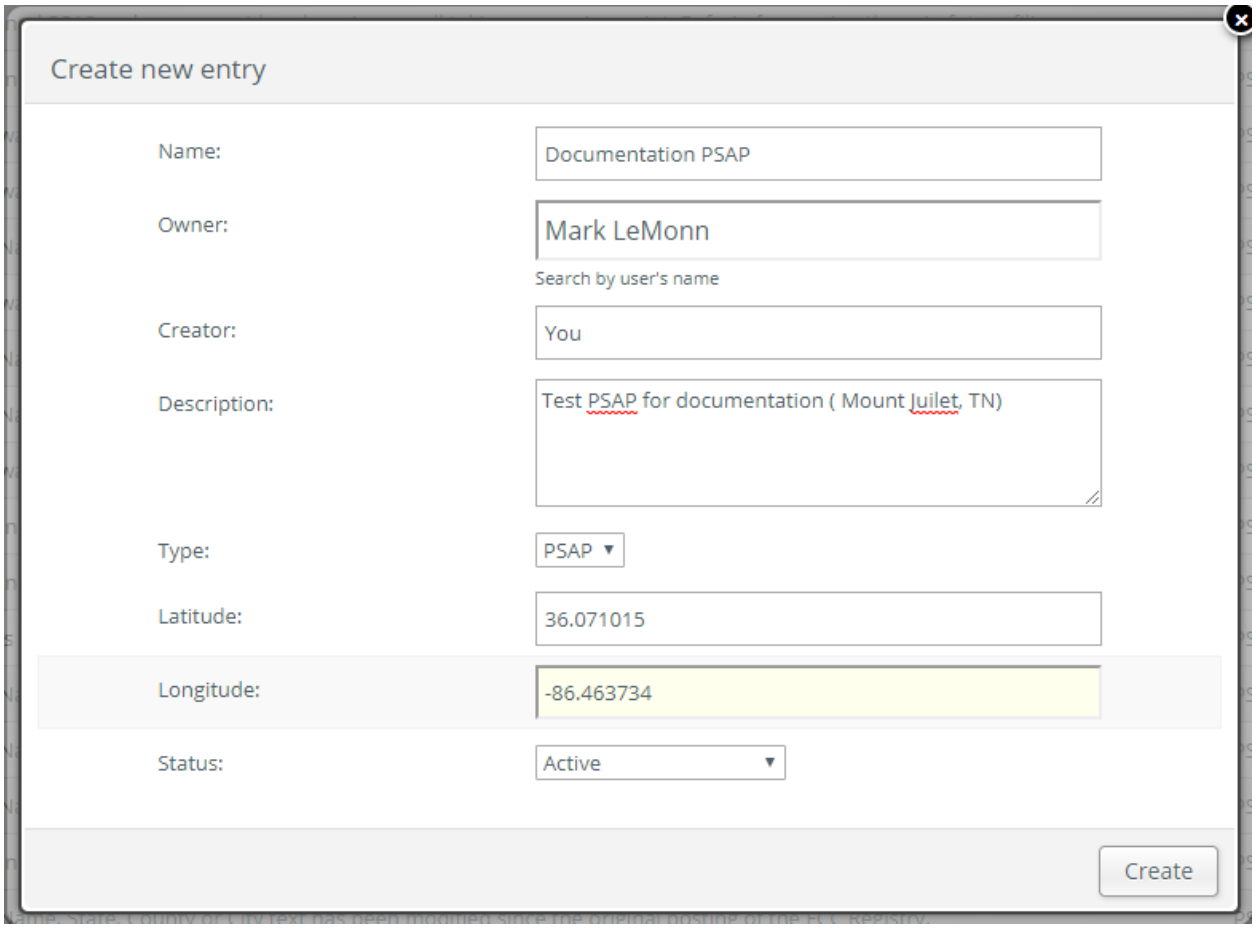


21. Click on the “ESInet Responsible Organization” link.

22. You will be routed to the “ESInet Responsible Organization” page. This is where you will create your PSAP or Responsible Organization.
23. Click on the “New” button at the top of the page.

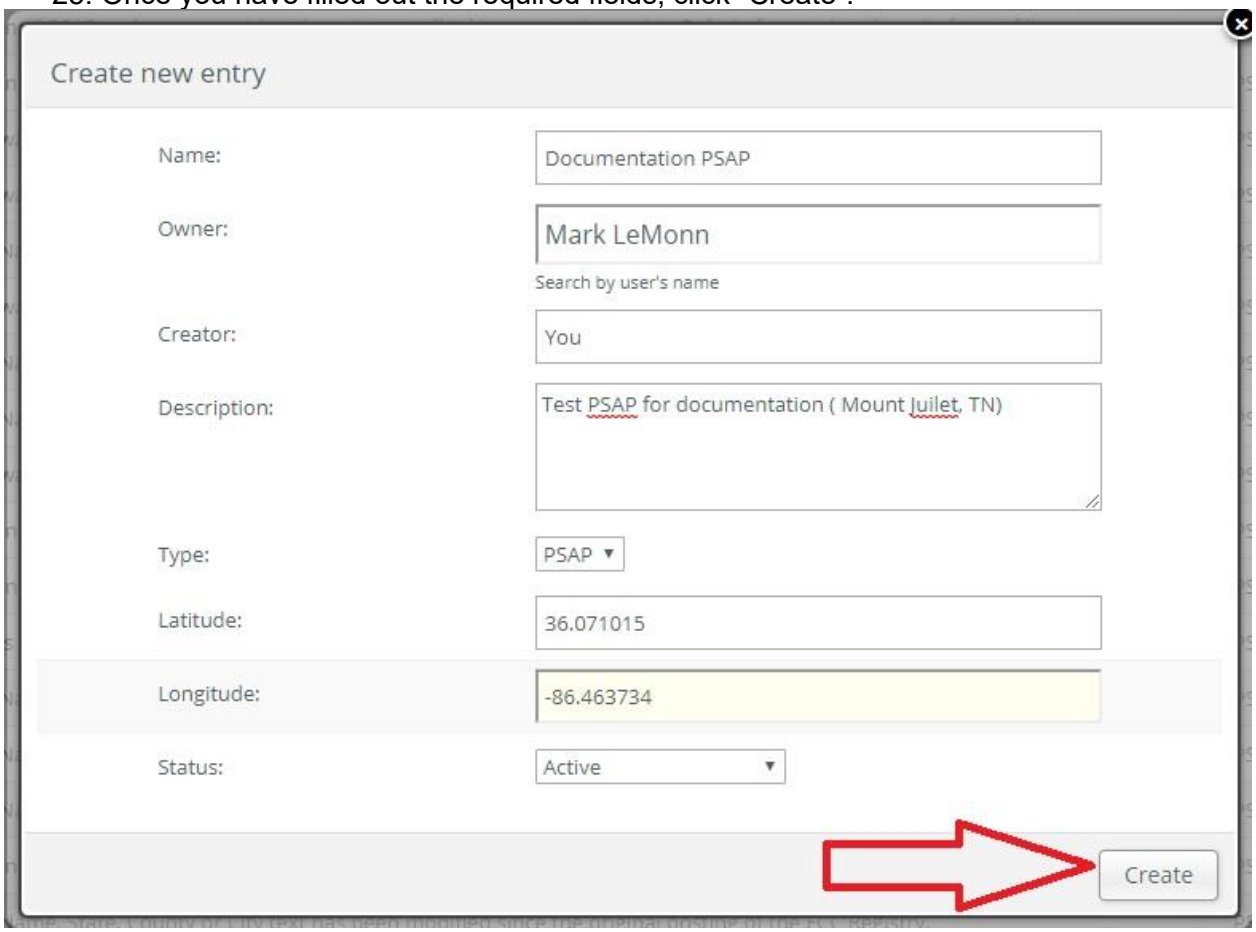


24. Once you have clicked on “New” a “Create new entry” pop up will appear. This is where you enter the Responsible Organization or PSAP information.

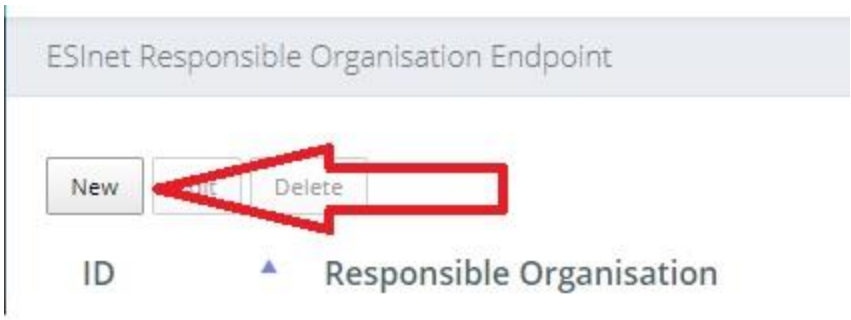


24a. Name - The Name of RO or PSAP
24b. Owner - Enter your name or the person that will be the owner of the PSAP. i.e. Don, Miguel, Mark, Ed, Alex, Shelly, etc….
24c. Creator - The default will be “you”.

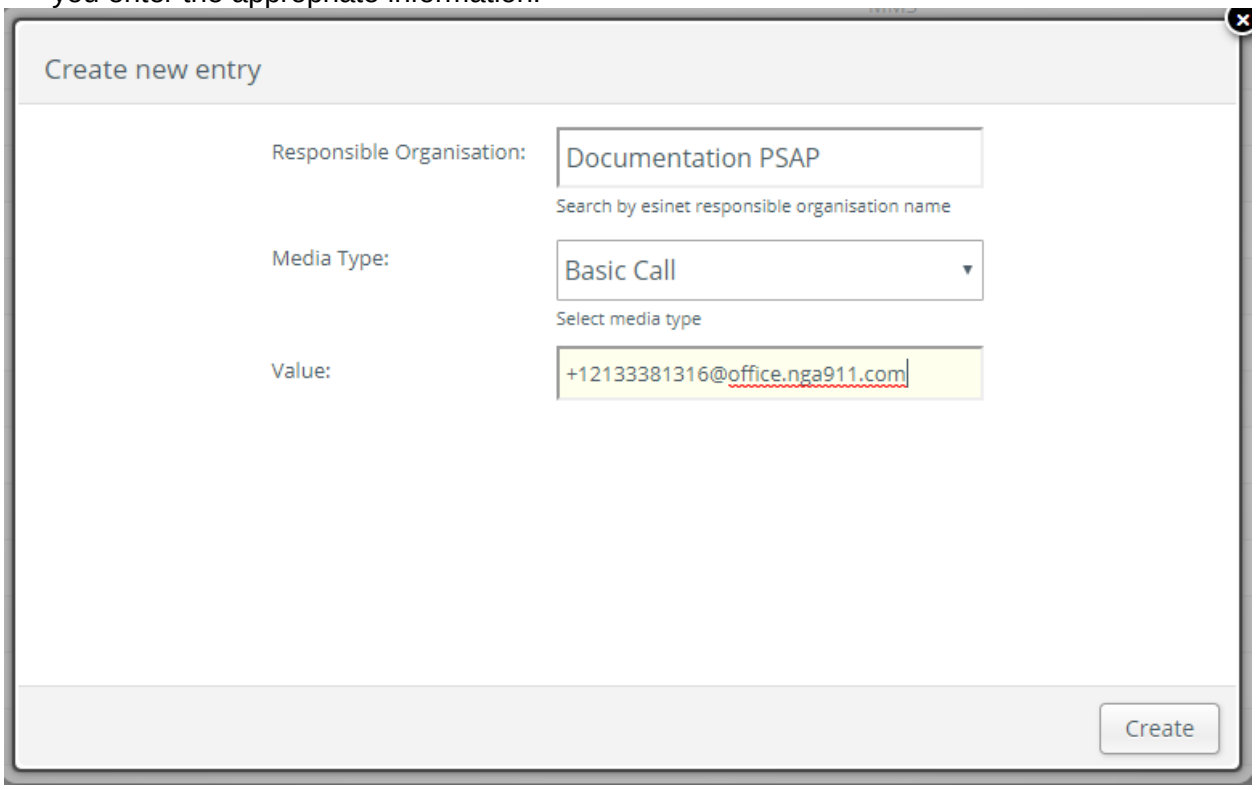
24d. Description - Enter a brief description of the RO or end point. (i.e. Mark PSAP test (Sacramento)
24e. Type - The default type is “PSAP”.
24f. Latitude - Enter the Latitude of the PSAP
24g. Longitude - Enter the Longitude of the PSAP
24h. Status - Active is the default choice of status. If you decide to choose “Inactive” or “Emergency Shutdown” you will not be able to route to the PSAP.
25. Once you have filled out the required fields, click “Create”.



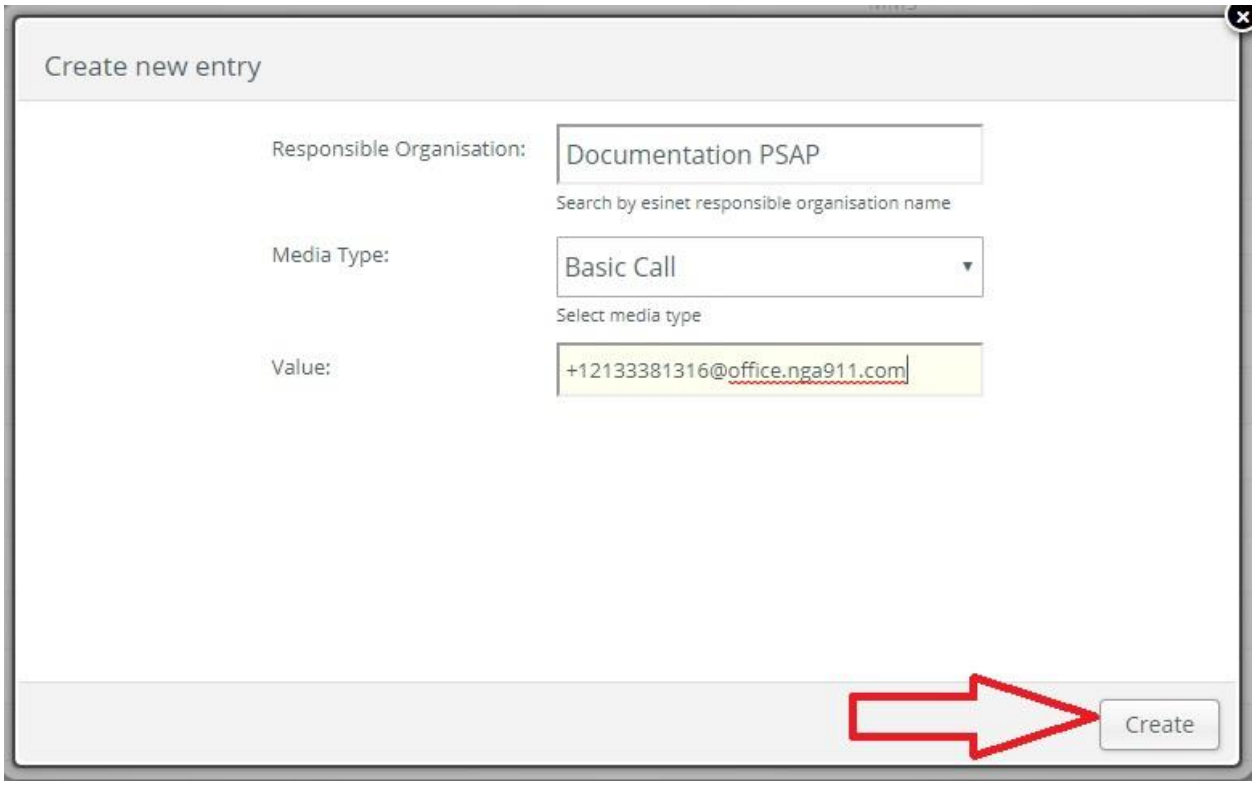
26. You have now created your RO.
27. Now that you have created your RO you must configure the endpoint. On the left side of the dashboard locate “ESInet Admin”, click on the arrow and locate “ESInet Responsible Organization Endpoint” and click on the link.
28. You will now be routed to the “Responsible Organization Endpoint” page. Here you will locate the endpoint that you created.
29. Click on the “New” button at the top of the page.



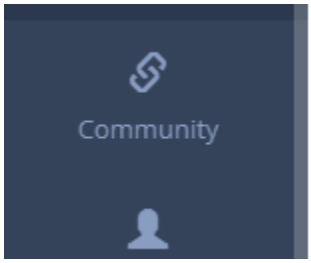
30. Once you have clicked the “New” button “Create new entry” pop up will appear. Here you enter the appropriate information.



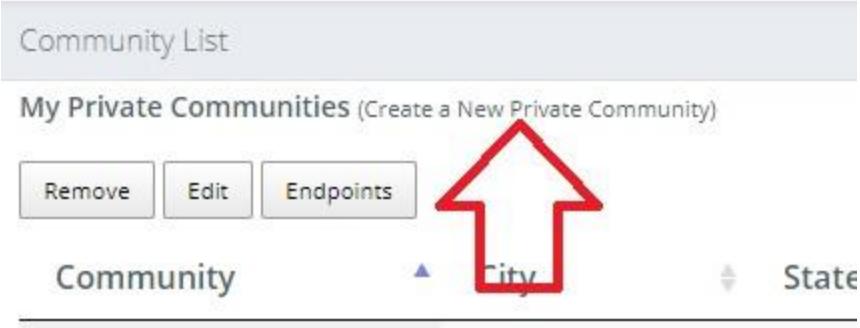
30a. Responsible Organization - Enter the name of the PSAP that will be the RO for the endpoint. I.e. Mark L PSAP, Dustin PSAP, Test PSAP, Palo Alto PD, Sacramento Sheriff, etc..
30b. Media Type - Select the media type that the Endpoint will be using to deliver the call, text or IM. Note, if the endpoint will be utilizing multiple media types you will be required to create an entry per media type.
30c. Value - Value will be the endpoint number or SIP number. I.e. +12133381316@office.nga911.com, +12133381316@dev.nga911.com, +12133381316@micro-auto.nga911.com
31. Once you have completed entering all of the required fields, click “Create”.



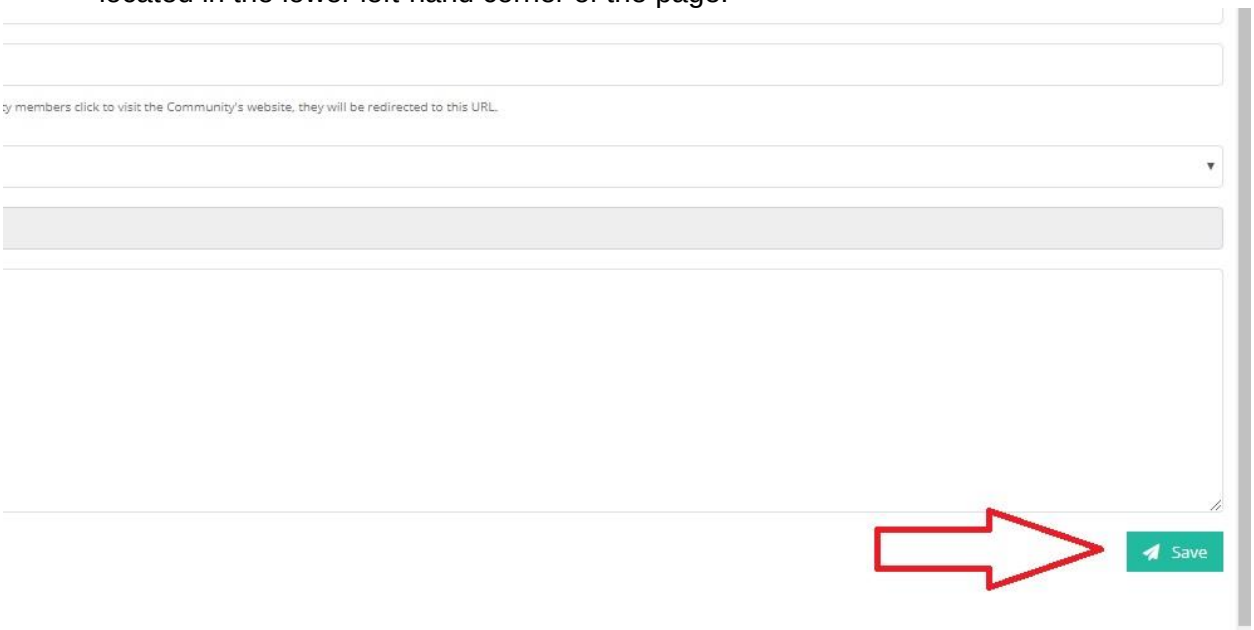
32. If you have multiple media types for the endpoint go back to line 29 to create each new media type. Once you have created all media types then you can move on.
33. Scroll down on the left side of the screen and locate the “Community” icon. Once you have located the “Community” icon, left click on the icon.



34. Once you have left clicked on the “Community” icon you will be routed to the “Community List”
35 . Once you have landed on the “Community List” page located the “Create a new private community” link. It will be located at the top of the page to the right of “My Private communities”
Left click on the link.

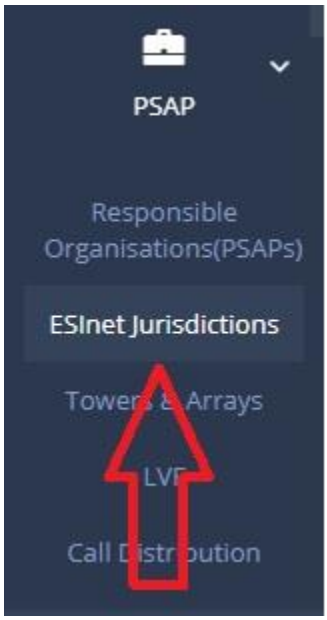


36. Once you have left clicked on “Create a New Private Community” you will be routed to the “Community” page. Here you can enter all the information for your PSAP or Endpoint.
36a. Name - The name of the PSAP or Endpoint. (At minimum this field should be completed, for testing purposes. If this is an actual PSAP or Endpoint that is live then more fields should be completed)
36b. Address - The address of the PSAP
36c. City - The city the PSAP is located.
36d. State - The State that the PSAP is located.
36e. Postal - The Postal code where the PSAP is located.
36f. Phone - The contact phone number of the PSAP
36g. Email - The email address of the contact of the PSAP
36h. Bank -
36i. Website redirect -
36j. Live Edit Design -
36k. External Website -
36l. Security - The Security level is based on the original configuration
36m. Owner - The owner is the person that created the endpoint
36n. Notes - Place any notes for the PSAP
37. Once you have completed all the required fields. Left click on the “Save” button located in the lower left-hand corner of the page.

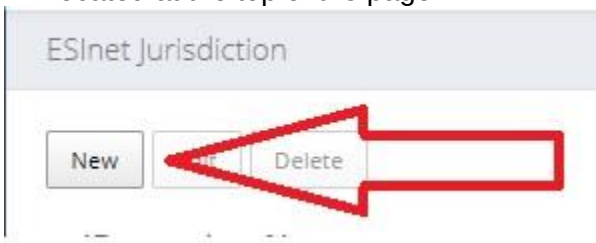


38. Once you have clicked “Save”. On the left side of the page, scroll up until you find the “PSAP” button, left click on the arrow.

39. Locate and left click on “ESInet Jurisdictions”

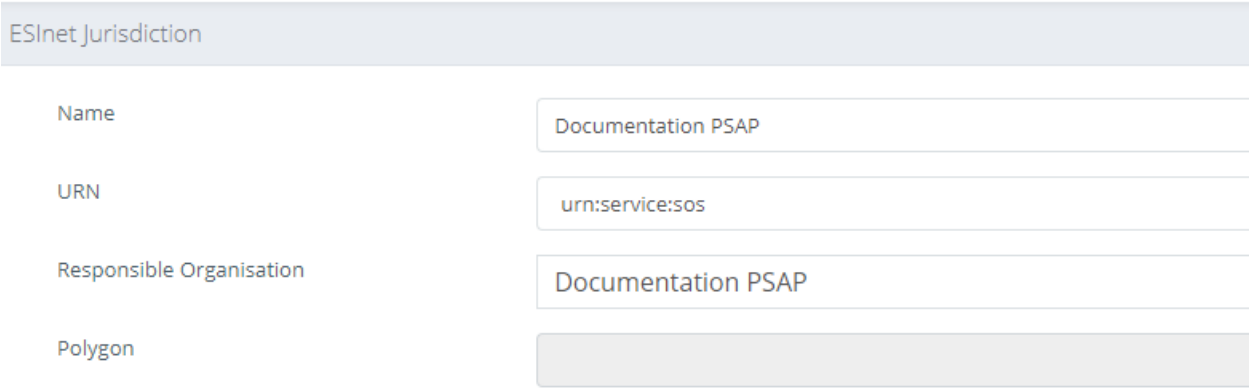


40. Once you have left clicked on “ESInet Jurisdictions” you will be routed to the “ESInet Jurisdictions” page. Locate and left click on the “New” button. The “New” button is located at the top of the page.

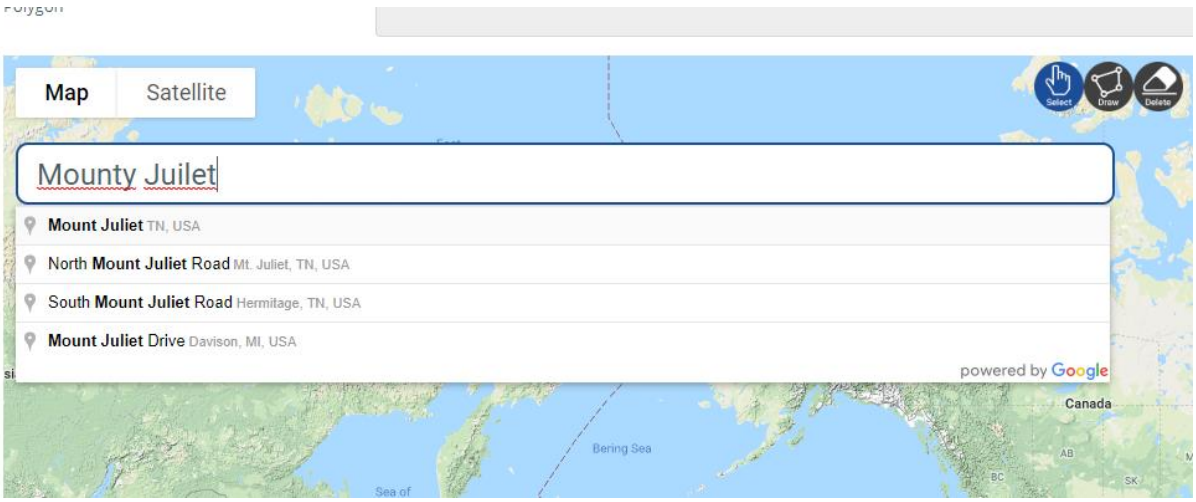


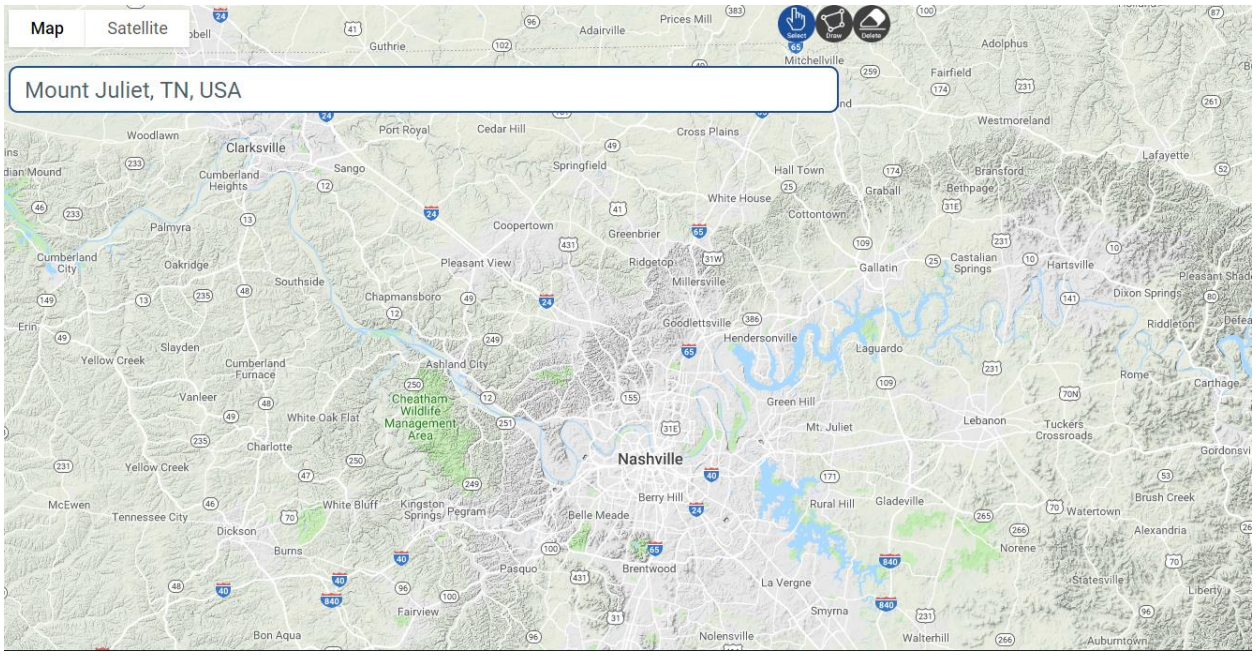
41. Once you have left clicked on the “New” button you will be routed to another “ESInet Jurisdiction”. This page is where you can set the PSAP boundaries and draw your polygon.

41a. Name - This is the location where you can enter the name of the PSAP.
41b. URN - The default URN is set to none. You can choose the URN by left clicking on the down arrow located to the right of the URN line. Set the URN to urn:service:sos.
42c. Responsible Organization - Enter the RO that will be responsible for the shape file. As you type the name of your PSAP or endpoint the page will present the available RO's that match your entry.



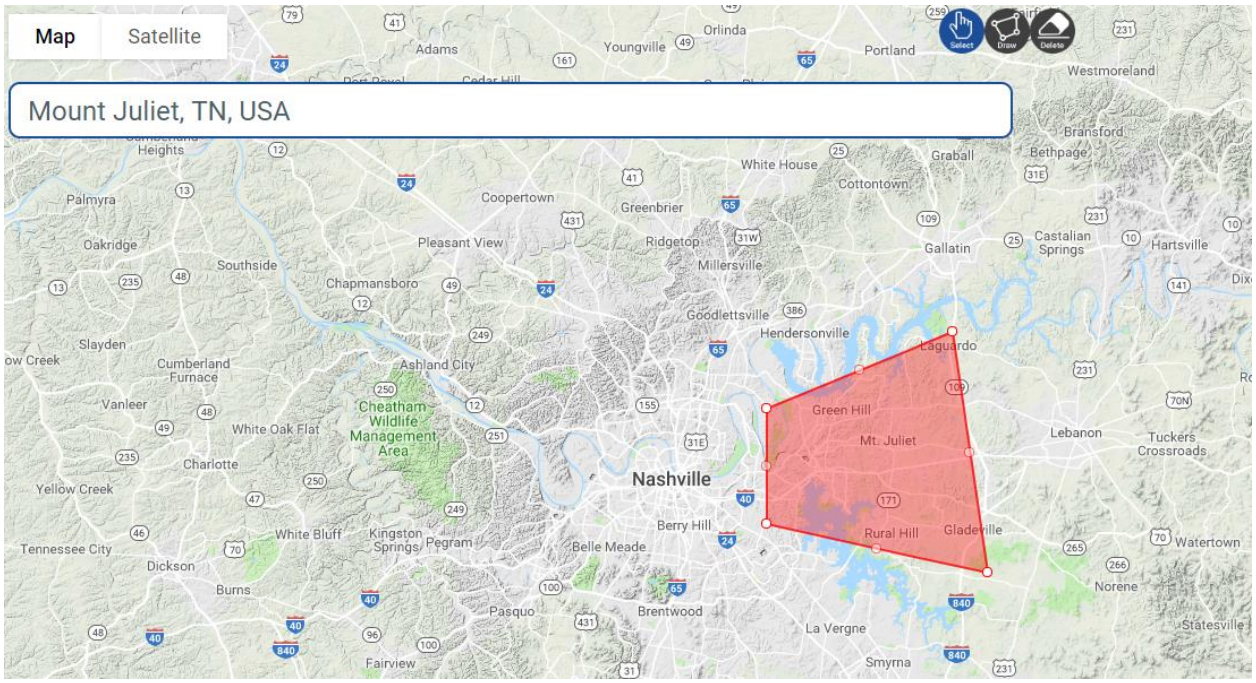
43. At the bottom of the page you can draw your shape file. If you know the city and state you can enter that into the search bar.





44. Once you have located the general area that you wish to draw your shape file. Left click on the draw icon. The Draw icon is located at the center top of the map.

45. Once you have clicked on the “Draw” icon you can click on the map to create dots. Before you complete your shape file make sure that all of the lines connect.



46. Once you have completed your shape file, left click on the “Create” button located in the bottom right-hand corner.
47. To verify that the PSAP, Endpoint and shape file works correctly plot your FakeGps location into the shape file and dial 911 from your android app. If the process was followed then you should reach your endpoint. If you do not reach your endpoint or route to the default endpoint please verify your profile, endpoints, and SIP account. If you are still unable to complete a call contact one of the system administrators.

ESInet Routes

11. Online Resources

NGA 911 has the latest version of training materials online. The credentialed personnel can log in to the secure Web-based portal.

- Online Resources including video training and tutorials
- Web User Interface Overview
- Teleconferences
- Business Resources
- Webinars
- Training PowerPoints
- Talking Points
- Support telephone number for the City, PSAP
- Maintenance and system(s) support training with NGA 911s
- A Support telephone number for the City is 877-899-8337 press #2 on the phone tree.
- Network/Monitoring/Help Desk
- Service Monitoring Tools
- Trouble Reporting

12. Disaster Recovery (DR)

Disaster Recovery

Disaster Recovery in the plan that will be followed if there is a service impacting incident such as a circuit cut. The TSP is notified and implemented by the NOC with direct communications to the service provider, the FCC, and of course to the State. If in fact all networks and data centers and redundant systems are down, we have the capability of bringing up new containers on other networks and cloud providers such as GCP and Azure. Restoration (if ever necessary) in the cloud is typified by the following Recovery Time Objects (RTO):

We notify the PSAP, the PSAP, the CPUC, the FCC and if necessary, the Nebraska National Guard of the need for circuits and connectivity including by temporary Cell on Wheels (COWS), LTE, MW, and Satellite.

Additionally, we will integrate our recourse/response plans with the PSAP and State NIMS and ICS protocols. Escalation procedures trigger notifications to operations and County, regional, state and Federal authorities of incidents and appropriate remedies for restoration. Escalation is

also used if the "Investigation and Diagnosis" and "Resolution and Recovery" are not resolved in a timely manner, notifying senior management to take necessary action to resolve any issues. Hierarchic escalation consists of two parts, one related to the technical efforts to restore the service (led by incident manager or a first-level operations technician and managed through a technical bridge), and the other related to NGA 911's communication management. There are different escalation paths for critical and non-critical incidents. For critical incidents, the appropriate managers from operations or from the State must be notified. Procedures are aligned to the National Incident Management System (NIMS) to facilitate coordination with public safety entities. These processes cover release management, business continuity, disaster recovery management, change management process, capacity management, national and local support structure for network configuration, maintenance and monitoring, protocols, and deployable assets for natural disasters.

NGA 911 recommends that the DR plan be tested with the PSAP on a quarterly basis to ensure that all functions work as designed. If there are any changes due to a Memorandum of Understanding (MOU) or an agreement between two or more PSAPs. Then the PSAP can schedule a test with NGA 911 to verify that new routes are functioning properly or as designed.

12.1 Service Restoration

NGA 911 regularly and routinely back's up configuration data and performs software upgrades in accordance with our DevOps Process. Previous working configurations can be invoked and loaded in parallel with the current release to test side-by-side performance on active-active systems. New functions and features are subject to a thorough and robust testing in pre-production environments. When code is ready for deployment the release process is structured to maintain the current load for a fixed period of time. Releases are made only on one copy of redundant deployments. The operational performance of new releases is continuously monitored to verify conformance with specifications. Any general release is completed when specifications are verified over a defined period. In an active-active environment, the performance of the new load is directly compared to the current load. In the case of an Operational Exception Fault (during Test Release and Full Release); Restoration or Fallback to previous version is automated so that both active-active instances are returned to the current stable release. These advanced practices ensure the State and the ESInet do not fall prey to the network failures due to poor release management which has befallen a number of PSAPs on a National Scale.

12.1 Iterative, Continuous Assessment DevOps Process

In order to maintain optimal, router, switch, and functional element configurations, NGA 911 adheres to the continuous assessment model depicted in the diagram above. Build types are characterized as being based on PSAP needs, on enhancements, and on Operational Necessity. Each type is coded in an Agile manner and integrated into the Test Environment. After successful testing, the releases are delivered in the parallel active-active manner described above. Utilizing the capabilities of our NOC/SOC software defined WAN; direct and immediate comparisons are made between the new load and current release. Performance is verified on a number of metrics including end-to-end jitter, latency, MOS fidelity, and call response times for

both. Any findings or measurements that fall out of the specified norm for the new release result in an automatic restoration to the current release.

The NGA 911 ESInet configuration tools provide version control and "rollback" functionality to all network elements. This allows the restoration of previous configurations or timely restoration of stored configurations in the event of equipment failure or disaster recovery.

Our network configuration management tools perform the following functions:

- Detect and report on configuration policy violations to provide compliance with corporate standards
- Utilize configuration templates and command templates, custom scripts, and configuration changes to provide consistent implementation of network configurations across similar site types
- Simultaneously modify configurations, change community strings, update ACLs, and block MAC addresses across many devices
- Compare start-up and running configuration files to troubleshoot device configurations issues
- Automatically check all network elements for changes and perform backup for all changed network device configurations on a daily basis
- Network configuration management tools have been implemented with geo diversity in place.

12.1 Outage Mitigation

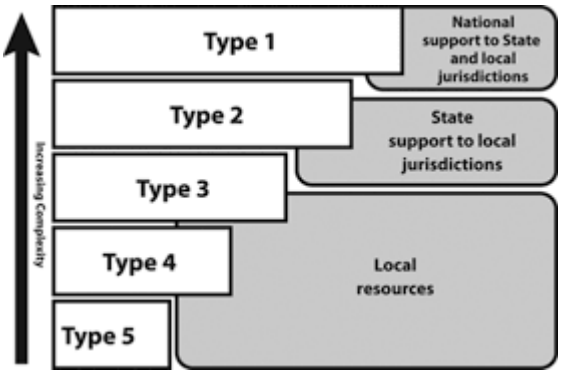
NGA 911 will create a Risk Mitigation Plan that is used for planning a complete risk monitoring and control system. The Risk Mitigation Plan evaluates identified risks and outlines mitigation actions. Included in this plan are the risk register, risk response plan tools and a risk matrix. The NGA 911 Project Manager collaborates with the Counties Project Manager/Sponsor to identify, assess and develop a response for existing any new risks throughout the project.

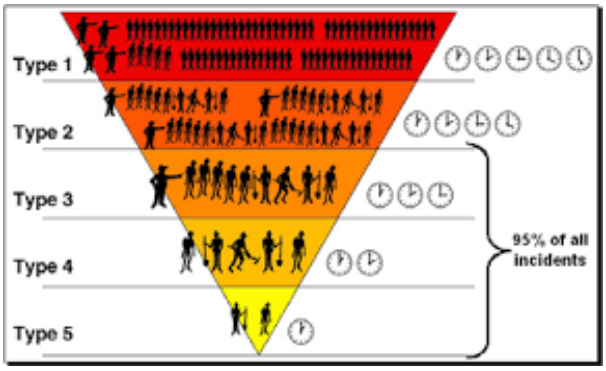
13. NIMS

The success of TP is dependent on the preparations made now during the project development and implementation phases. This section details how PSAP SEMS-NIMS Integration and the COOP are incorporated into the DR operational processes.

These processes are based upon the FEMA NIMS Incident Types where the number of people activated and the length of the response are identified by Type where the lower the number reflects a larger incident(s). This does not necessarily mean that more NGA 911 personnel are involved for any incident Type, but the overall personnel and organizations in a city, municipality, county, region, State, Federal and interstate that are brought to bear on the Incident(s). Nonetheless the Nebraska 9-1-1 System and the Alert and Warning System

(amongst others) become a significant and critical part of the whole. For this reason, the NGA 911 DR is directly tied to NIMS and SEMS (see Section X below).





The NIMS Types are applied as the Incident(s) ensues. But prior to an Incident/Event, we must also consider the NIMS Activation Levels.

Activation Level	Description
3 Normal Operations/ Steady State	• Activities that are normal for the EOC when no incident or specific risk or hazard has been identified • Routine watch and warning activities if the EOC normally houses this function
2 Enhanced Steady-State/ Partial Activation	• Certain EOC team members/organizations are activated to monitor a credible threat, risk, or hazard and/or to support the response to a new and potentially evolving incident
1 Full Activation	• EOC team is activated, including personnel from all assisting agencies, to support the response to a major incident or credible threat

The Activation Levels distinguish between Normal, Enhanced, and Full for an EOC. NGA 911 adopts and these distinctions in our COOP and adapts them into 4 categories: Normal, Elevated, Alarm, and Recovery which is are detailed in Section 2.1.2.

a. Web-based Portal

Continuity of Operations (COOP) is the initiative that ensures that the NG9-1-1 system, services, and features supplied to PSAP by NGA 911 are able to continue operation of essential functions under a broad range of circumstances including all-hazard emergencies as well as natural, man-made, and technological threats and national security emergencies. Today's threat environment makes COOP planning even more critical. The components of the COOP cover:

- Operational Processes
- Recovery Processes

- Communications
- Training
- NGA 911 Contact Lists
- Service Provider Contract Lists
- Priority Services
- Alternate Operations Site

13.1 Recovery Processes

The operational processes emphasize interfaces, recovery processes deal with the specific element or interface impacted by failure. In this case each and every functional element and interface in the system are subject to performance and tolerance monitoring and analysis. The ideal is to maintain every one of them in tolerance 100% of the time. In this respect we look at performance from the following levels:

1. Component
2. Capability
3. Application
4. Function
5. Failover
6. End to End

A modification of the NIMS Activation States, at each level we have procedures to assess, repair/restore, and failover so as to maintain above all others number 6 the end-to-end performance of the network. Assessments of the condition of the network are based on a Triage Table Maintained by Technical Operations.

N = Normal
E = Elevated
A = Alarm
R = Recovery

Normal operations are those in which the tolerances for End to End performance and Failover and/or when redundant processes and systems in place provide for operations at a nominal 99.99%

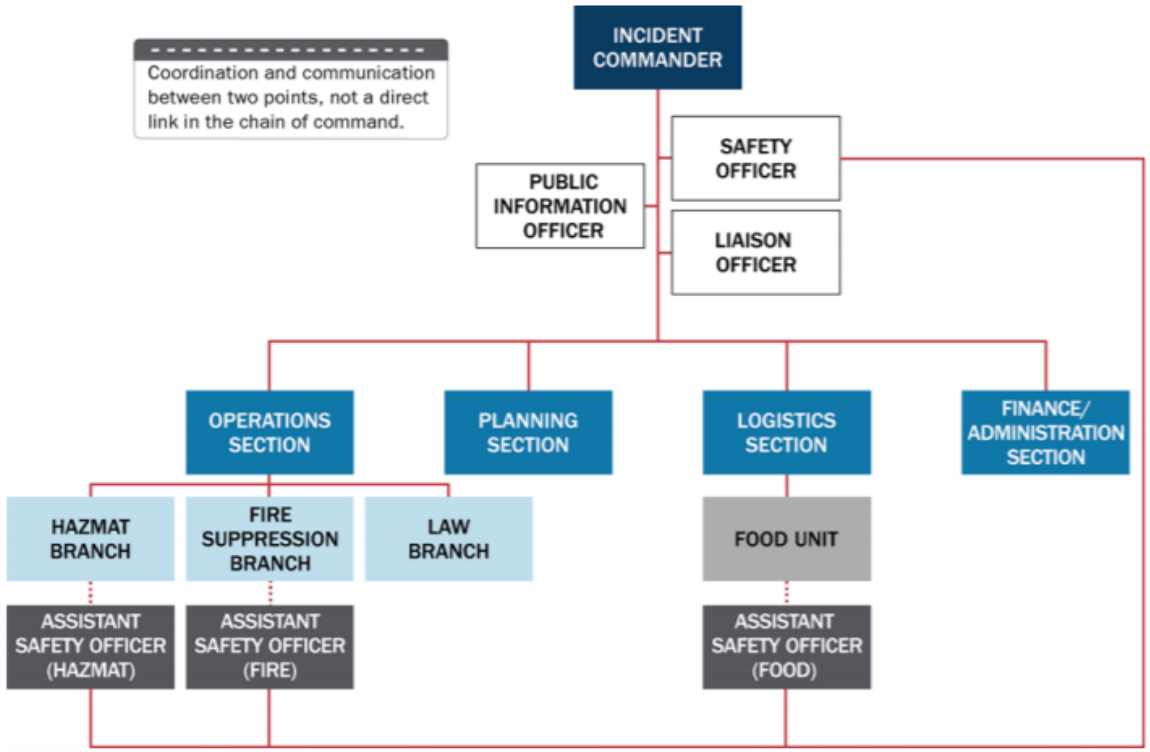
Elevated Operation are those in which the tolerances for redundancy (measured in real-time) are at or approaching 99.9%

Alarm conditions are those in which End to End performance or any singular/aggregate service is operating in a non-redundant state.

Recovery is when the singular or aggregate failure of a system or systems has significantly degraded or outright terminated a 9-1-1 service from one or more OSPs to one or more PSAPs.

13.2 Communications Response Team

The key to effective response is a Communications Response Team (CRT) with clearly defined roles and responsibilities. The NGA 911 CRT is loosely modelled on the NIMS structure:



From this model we derive the corresponding team members/roles to effectively respond to a disaster. The following individuals will be identified. In a future version of this table the roles will also be assigned by shift and geography so that most roles will have at least one primary and one secondary individual (taking vacations and holidays into account) and many of the Coordinator roles will have up to three people assigned each to cover an 8-hour shift.

Role	Name	Number	Email
DR Manager			
DR Technical Manager			
Trunk Services			
Aggregation Services			
Core Services			
Interfaces			
NOC Manager			
Field Services Manager			

SOC Manager			

DR Communications Manager has overall responsibility for managing and communicating the current conditions, expected actions and responses, and estimated restoration times.

DR Technical Manager has responsibility for Triage, Tier I Troubleshooting, identifying required resources, and managing those resources to bring about service restoration.

Trunk Services is responsible for the troubleshooting and restoration of trunk services.

Aggregation Services is responsible for the troubleshooting and restoration of aggregation services.

Core Services Coordinator is responsible for the troubleshooting and restoration of core services.

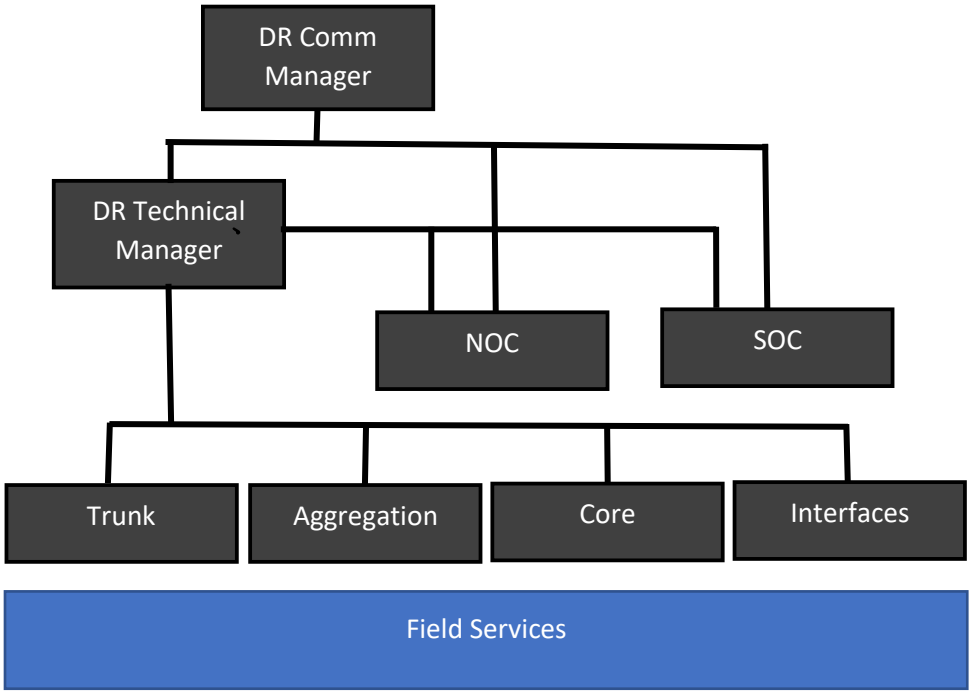
Interface Coordinator is responsible for the troubleshooting and restoration of interfaces.

NOC Manager has responsibility for the management and coordination of the OSS including NMS, Reporting, Troubleshooting, and coordination of the Field Services organization. The NOC manager reports to the DR Manager and provides resources to the DR Technical Manager and the Service Coordinators.

Field Services Manager manages the required field services at the direction DR Technical Manager with support from the NOC Manager.

SOC Manager is responsible for assisting the Service Coordinators for restoration of services due to cyber and security attacks, malware, etc.

The lines of communication within the DR support teams are depicted in the diagram below. In preparation for a potential disaster or in response to a spontaneous disaster, the DR Communications Manager is activated. The Communications Manager is in immediate and constant communication with the NOC and SOC through dashboards, messaging (IM), and telephone. The NOC reports up the current condition of the network and what actions have and are being taken to restore operations. A key part of restoration is the Triage work performed by the DR Technical Manager. The Technical Manager has access to the dashboards and the OSS which is made up of the Network Management System (NMS) and the assessments and reports being made by the active technical teams. It is the Technical Manager who decides which Technical Coordinators need to be activated depending on the location and type of disruptions are impacting the network. Actions that require field support from NGA 911 are run through the Field Services Office.



2.1.4 Employee Training Exercises

Disaster Recovery (DR) Training is divided between internal training on this the DR Framework and additional Training Requirements depending on role and responsibility.

General DR training for all members of the staff supporting the Region and subcontractors covers the following topics:

- Introduction to the Disaster Response Plan
- Statement of the goals and objectives.
- Alignment with PSAP 9-1-1 Branch Strategies
- Alignment with PSAP COOP and SEMS
- Strategies, tactics, policies, and constraints affecting the DR Plan.
- Organizations, activities, and interactions among participants and stakeholders.
- Processes for initiating, developing, maintaining, and upgrading (enhancing) the DR Framework.

The first course will be drafted and signed off on by PSAP once an Approved Disaster Recovery Plan is finalized which NGA 911 anticipates being in the 2nd Quarter of 2020.

NIMS Training

All members of NGA 911's staff directly involved in DR will also take FEMA's IS-700: National Incident Management System, An Introduction course online.

Table Top Exercises (TTX)

Once the DR plan is formalized and approved (2nd QTR 2020), NGA 911 will design and implement a series of table top exercises (TTX) in order to exercise and test the applicability of DR plans. These TTX's will cover the full range of possible events from anticipated to sudden and exercise scenarios typical of the kind of failures that can be anticipated at the aggregation, trunking, core, PSAP, and interface levels (and combinations thereof). It is expected that a review of the TTX may result in the modification of Processes, Procedures, Roles, Communications Trees, Response and Recovery Techniques, if necessary. Changes to the plan will be reflected in the Training Documents and previously trained individuals will be required to complete any supplemental materials within 30 days of formal changes to the DR Plan.

After Action Reports (AAR)

Once in place the DR Plan is subject to modifications and improvements. This is especially true after an event or events that result in the triggering and implementation of the DR Plan. Such events will result in an assessment of the response measured against the plan in place at the time and corresponding SLA's. A corresponding after-action report (AAR) will be produced and recommendations made to any change in Processes, Procedures, Roles, Communications Trees, Response and Recovery Techniques, if necessary.

2.1.5 Disaster Recovery (DR) Leadership Training

NGA 911 will also develop in concert with PSAP DR Leadership Training for the DR Communications and Technical Managers designed to align NGA 911's DR Plan with the overall Framework adopted by PSAP.

NGA 911 at this time is looking into the DR Leadership attending FEMA's E550 Continuity of Operations (COOP) Planning Course in XX date, 20XX; depending on availability, and eligibility based on prerequisite courses, certifications, and qualifications.

2.1.6 Employee Contact Lists

Key Points of Contact

- NG9-1-1 Project Coordinator – Kim Aleman
- NG9-1-1 Trunk Services Coordinator – Miguel Martinez
- NG9-1-1 Aggregation Services Coordinator – Mike DeWeese
- NG9-1-1 Core Services Coordinator – Ed Vea
- NG9-1-1 Prime Functions and Services Coordinator – Kim Aleman
- System Monitoring and Outage Reporting Coordinator – Mark LeMonn
- Escalation Manager – Michelle Bland, ENP

- Training Manager – Shelly Guenther, ENP

14. System and Service Availability

NGA 911 has a High Availability (HA) design Next Generation 9-1-1 Core Services (NGCS).

14.1 Network Monitoring

The NGA 911 Service Management Center within our Network Operations Center (NOC) monitors the ESInet network 24/7/365 to ensure impairments are rapidly addressed.

● Expert Monitoring systems give an intuitive view so that personnel can react quickly even to hints of impairment.

● The NGA 911 NOC is equipped with a Network Management System (NMS) that monitors the performance of the network and infrastructure of the State's NG9-1-1 system 24/7/365.

● The NGA 911 NOC continuously monitors the performance and availability of all devices.

● The NGA 911 NOC monitors network performance, including throughput, latency, jitter, packet loss, and other key SLA parameters.

● The NGA 911 SOC monitors the network for network intrusion attempts or security breaches and be capable of issuing security alerts when an event is recognized.

● The NGA 911 NOC create alarms based on thresholds and parameters and distribute alarm notifications appropriately.

● The NGA 911 NOC monitors the environment at all data centers or points of presence where critical network components are housed to ensure functionality.

● The NGA 911 NOC monitors ancillary network components such as power utilization and backup power systems.

NGA 911 operates a NOC that manages PSAPs in multiple jurisdictions around the country. The NOC conforms to our Quality Management System (QMS) and is tied together by a comprehensive Network Management System. Below is an overview layout of the NMS interworks, monitors, analyzes, and provides an executive dashboard display for the complete network, and the physical and virtual functional elements of the NGCS.

14.2 Alarming

NGA 911 provides near real-time alerts when the monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by service and Security teams. NGA 911 correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis. Upon assessment and discovery of risk, we disable accounts that display atypical usage matching the characteristics of bad actors.

Our Security team extracts all log messages related to system access and provides reports to designated officials. Log analysis is performed to identify events based on defined risk management parameters. Through monitoring of all Functional Elements, NGA 911 will be able to quickly identify and respond to alarms and network events in the network. If an alarm or network event occurs NGA 911 will complete a root cause analysis on the condition to determine an effective, long term solution. NGA 911 will identify the symptoms of the problem and implement the appropriate corrective action to improve safety and reliability going forward. NGA 911 is ready and equipped to resolve problems so that 9-1-1 operations can continue without disruption.

Additionally, on the OSS, NMS, and NOC side; The technology deployed end-to-end by NGA 911 appends flow tracing packets to each and every packet traversing the entire ESInet from ingress to egress whether signaling or media. These "sidecars" are used to measure latency, jitter, route, bandwidth and travel times for each and every route and interconnect service provider on the ESInet. This data is fed directly into the NGA 911 monitoring systems and logged for real-time alarms and historical SLA verification and auditing.

There are several top categories of alarms that will be setup on the initial dashboard screen to be able to fit them on a reasonable amount of screen space. The user can view each item in real-time (updated every second) or view their historical data in 1 hour, 4 hours, 1 day, and 7-day increments over a user-specified date range). The statistics data in different categories can also be exported to a CSV file for additional data analysis. PDF reports can also be generated.

14.3 Maintenance

NGA 911 provides 24 hours a day, 7 days a week, 365 days a year (24/7/365) maintenance support for the life of the service-based solution. NGA 911 customers will receive Help Desk and technical services support for all products and services included in NGA 911's proposed solution. As part of our comprehensive maintenance and support program, we provide monthly reports on the health of the systems in addition to 24x7 monitoring.

The State PSAPs and Management can obtain information, updates, and status of service/maintenance issues, account information, including but not limited to the reporting system. NGA 911 understands the Public Safety Maintenance windows and associated notification processes. NGA 911 will perform necessary maintenance during the standard Public Safety Maintenance Window of Midnight - 4:00 A.M. Monday - Thursday. However, NGA 911 will work with the State and PSAP to pre-define the Public Safety Maintenance Window if the standard NGA 911 Public Safety Maintenance Window is not conducive to PSAP operations.

NGA 911 Operations Staff will make advance notification of planned network outages that may impact the PSAP. Notification will be made a minimum of 24 hours in advance via email. NGA 911 Operations Staff will confirm receipt of notification received prior to beginning maintenance procedures/processes.

The State and PSAPs can obtain information, updates, and status of service/maintenance issues, account information, including but not limited to the reporting system by calling the support number.

- The maintenance support number is 1-877-899-8337 x 2.

NG9-1-1 maintenance support includes:

- Troubleshooting:
  - 24/7/365 Support Telephone Number
  - Web User Interface
  - Service Monitoring Tools including Dashboards
  - Network/Monitoring/Help Desk
  - Trouble Reporting including Outage and Trouble Ticket Reports
  - Preventative Maintenance
  - Tiered maintenance and Support System through the NGA 911 Network Operations Center (NOC)
  - Escalation Support

In the NGA 911 Network Operation Center/Security Operation Center we adhere to the following processes:

Network and System Event Logging (E1); Change Management Processes and Procedures (J); Configuration Backup and Restoration (L).

In accordance with FCC guidelines, NGA 911 formulates plans and implements strategies that ensure the continued operation of facilities before, during, and after an incident. The main steps of our DR plan are ***preparation***, ***response***, and ***recovery***.

- Critical Interfaces include:
  - Aggregation to PNSP / RNSP and OSP Interface
  - PNSP / RNSP ESInet interface
  - PSAP Interface
  - SD WAN Interface
  - System Monitoring Interface

Form A
Bidder Proposal Point of Contact
Request for Proposal Number 6264 Z1

Form A should be completed and submitted with each response to this solicitation. This is intended to provide the State with information on the bidder's name and address, and the specific person(s) who are responsible for preparation of the bidder's response.

Preparation of Response Contact Information	
Bidder Name:	NGA 911, LLC
Bidder Address:	8383 Wilshire Blvd, Suite 800 Beverly Hills, CA 90211
Contact Person & Title:	Michelle Bland, Senior Vice President, Operations
E-mail Address:	Michelle@nga911.com
Telephone Number (Office):	(303) 898-1794
Telephone Number (Cellular):	(303) 898-1794
Fax Number:	(818) 487-1464

Each bidder should also designate a specific contact person who will be responsible for responding to the State if any clarifications of the bidder's response should become necessary. This will also be the person who the State contacts to set up a presentation/demonstration, if required.

Communication with the State Contact Information	
Bidder Name:	NGA 911, LLC
Bidder Address:	8383 Wilshire Blvd, Suite 800 Beverly Hills, CA 90211
Contact Person & Title:	Darold Whitmer, Senior Vice President, Strategic Relations
E-mail Address:	Darold@nga911.com
Telephone Number (Office):	(303) 898-1794
Telephone Number (Cellular):	(303) 898-1794
Fax Number:	(818) 487-1464

Form B
Notification of Intent to Attend Pre-Proposal Conference
Request for Proposal Number 6264 Z1

Bidder Name:	NGA 911, LLC
Bidder Address:	8383 Wilshire Blvd, Suite 800 Beverly Hills, CA 90211
Contact Person:	Darold Whitmer
E-mail Address:	Darold@nga911.com
Telephone Number:	(303) 898-1794
Fax Number:	(818) 487-1464
Number of Attendees:	3

The "Notification of Intent to Attend Pre-Proposal Conference" form **should** be submitted to the State Purchasing Bureau via e-mail (as.materielpurchasing@nebraska.gov), hand delivered or US Mail by the date shown in the Schedule of Events.

Anne DeGraff, PMP

NGA 911 Project Resume

Role

Hosted Call Handling Project Manager responsible for the overall planning and implementation of the Hosted Call Handling services.

Responsibilities

Responsible for developing and executing Hosted Call Handling project plans, integrated timelines, work breakdown structures, communication plans, risk mitigation plans and post-migration service plans.

Experience

• Experience includes over 40 years in the computing and communication fields with over twenty-five years managing complex technical as well as Public Safety projects – Qwest/CenturyLink, Intrado/West Safety Services.

• Excels in organizing, planning, scheduling and successfully delivering on challenging multi PSAP and vendor deployments. Expertise in Program Management, Project Management, Customer Relations, Strategic Planning and Execution as well as Team Building.

• Responsible for managing all key Hosted Call Handling activities including Organization Alignment, Governance Framework Implementation, Inventory Assessment, Site/End User Engagement, Asset Alignment, Solution Assessment, Agency Planning, Operations Planning, Transition Planning, Sustainment/Ongoing Operations Approach and Continuous Service Improvement Model Development as well as Implementation Execution.

Certifications/Credentials

• Project Management Professional (PMP) Certification – Project Management Institute

• Program Manager Certification – University of Denver

• Technical Level 3 Project Manager Certification – U S WEST IT Center for Project Management

• Yellow Belt Certification – Lean Six Sigma Institute Education

• Bachelor of Arts, Education – University of Northern Colorado, Greeley, CO

Michelle Bland, ENP, CMCP, MBA

Experience

4/2018 – Current NGA 911, L.L.C. Sacramento, CA

Senior Vice President, Operations

- Review plans, proposals, and other IT/Telecommunications project documents to ensure effectiveness and efficiency, feasible alternatives, project merits, and proper planning
- Manager responsible for spending plan, budgets, and procurement
- Develop business specifications
- Identify security requirements
- Project manage large scale projects both National and International
- Develop business processes and procedures
- Develop project plans and timelines
- Manage Help Desk, Project Management, Technical Support, Administrative Support

8/2017 – 4/2018 California Department of Technology Sacramento, CA

Procurement Manager (Information Technology Supervisor II)

- Review plans, proposals, and other IT/Telecommunications project documents to ensure effectiveness and efficiency, feasible alternatives, project merits, and proper planning
- Manager responsible for spending plan, budgets, and procurement
- Develop formal and informal procurements including IFB, RFP, RFQ, and NCBs
- Develop business specifications
- Identify security requirements
- Develop project plans and timelines
- Analyze department requests for special requirements for technical specifications for completeness and accuracy

6/2007- 8/2017 California Highway Patrol Sacramento, CA

9-1-1 Program Manager (Telecommunications Systems Manager I Supervisor)

- Administrator of the Wireless 9-1-1 Program for the California Highway Patrol through standards, contracts, and guidelines
- Identify and perform technical analysis, and evaluate equipment, systems, and services for 25 9-1-1 dispatch centers
- Manager responsible for spending plan, budgets, and procurement
- Facilitate the reconciliation and resolution of supplier/state concerns relative to technical and administrative requirements while maintaining competition in accordance with State and Federal laws relating to procurement and contracts and utilizing a personal computer, relate software applications, and various office and communication equipment
- Collaborate with staff, management at every level, other State departments, vendors, and local Public Safety Answering Points
- Serve as project leader and skilled consultant to Executive Management. Represented the California Highway Patrol as a subject matter expert, technical advisor, facilitator, and/or member of any task force, committee, advisory group, or project team relevant to 9-1-1 communications
- Test and evaluate features, performance, and technical attributes of products, equipment, and services for implementation

- Perform cost comparisons and cost/benefit analysis. Compiled and submitted information for budget change proposals, write justifications, initiate or amend grant proposals
- Assist departments and agencies with issues concerning 9-1-1 operations, telecom equipment, personnel, and training programs relative to the Wireless 9-1-1 Program, and Texting to 9-1-1
- Reviewed and validated all operational requirements for system compliance
- Project Managed multiple large projects concurrently as they impacted the 9-1-1 dispatch center

Education/Certification

ITIL Foundation Certified 6/2016

Roger Nicholls

9 Deer Creek Ln, Laguna Hills, Ca 92653
714-270-2825 | rogernicholls@cox.net

Professional Summary

Skills & Abilities

Expert understanding of Multiple 911 systems previously used to many of the latest Next Generations systems.

Complete repair services on all 911 platforms

Experience

01/1980 to 03/2020

Communications

Supervised Installation and Repair Team of E911 equipment. Installed and maintained various 911 systems

Supervised E911 Service Team for Frontier Communication for 4 Years

- Worked with E911 Systems to resolve all Telecommunications problems, improve operations and provide exceptional customer service.
- Increased customer satisfaction and repeat business through relentless pursuit of resolutions to problems arising from E911 Service, protecting the company reputation and loyal client.

Shelly R. Guenther, ENP Shelly.Guenther@NGA911.com 877-899-8337 ext 5911

TECHNICAL AND PROFESSIONAL EXPERTISE

● Six Sigma Green Belt ● Scrum Fundamentals Certified ● Scrum Product Owner Certified ● Emergency Number Professional (ENP)

SR. PROJECT MANAGER – *NGA 911* 08/2018 – Present

- All aspects of Project management, Scrum Product Owner, documentation, customer meetings.
- Tariff writing, technical document management.
- Managing state procurement.

CLASSROOM ASSISTANT – *Centennial Elementary* 09/2017 – 05/2018

- Tutored individual students 1:1 and 1:8 with emphasis in math and reading.
- Interacting with children to support learning and communicated professional and effectively with staff.
- St. Vrain Instructional Technology Advisory Representative working with district CTO.

VP STRATEGIC ACCOUNTS / PRODUCT LINE MANAGER – *911 Datamaster* 12/2016 – 08/2017

- Customer relations and sales to large U.S. Government (USG), key customers, and Public Safety Answering Points (PSAP) strategic accounts.
- Conducted market research and competitive analyses.
- Managed Scrum team build and backlog, entire business development lifecycle management for enterprise market geospatial esri GIS software QA/QC tools contributing to the vision and overall architecture roadmap.
- Responsible for Technical Overviews and customer demos. Implemented process flow.
- Work directly with other product owners, system engineers, program managers, developers, project managers, testers, and customers to define product offering.
- Created go to market business plans with annual and multi-year product line objectives and strategy.

SR. PRODUCT LEAD / GLOBAL ACCOUNT MANAGER – *CenturyLink* 06/2007 – 10/2016

- $200M project SaaS. Implemented Hosted customer premise equipment (CPE) workstations in the Cloud, analyzed results, quality control, and managed lab priorities for 9-1-1 CPE upgrades.
- Core team member for complying with the FCC Consent Decree, assisted Legal and Regulatory.
- Subject matter expert (SME), support key sales opportunities recommending solutions that satisfy business needs, support the product roadmap, and support strategic, tactical, and customer driven enhancements.
- Instrumental in resolving conflict by highlighting rules and regulations, resulting in consensus and resolution.
- Worked with PUC, PRC, Homeland Security, and national organizations to identify roadblocks and create roadmap to resolve. Negotiated and managed vendor contracts.

DIRECTOR – *Vonage* 09/2005 – 04/2007

- Drove growth of $184M in new rate centers due to successfully marketed product to untouched demographics.
- Coordinated statewide and regional deployments, planning engaging Governors, PUCs/PRCs.
- Managed strategic accounts and vendors for 9-1-1 database migration.
- Interfaced with Public Safety Answering Points (PSAP)s, Local Exchange Carriers (LECs), VoIP Positioning Centers (VPCs), CLECs, 3rd party providers, state and local agencies. Directed activities in rulemaking, leadership in 911 Taskforces, Colorado 911 Resource Center, and other national organizations.
- Created and delivered compelling presentations via in-person meetings, conferences, phone and web.

PROJECT MANAGER / PUBLIC SAFETY LIAISON - *West Corp.* 10/2000 – 06/2005

- Ensured project stayed on track and monthly goals were met. Conducted acceptance testing on live 9-1-1 systems. Trouble shot issues with deployments. Managed change management requests.
- Speaker at National, Regional, local NENA and APCO conf. Developed and delivered training.
- Single Point of Contact for our Wireless customers. Prepared and submitted annual budgets.

- Project managed and deployed carrier 9-1-1 routing for Tier 1 and 2 Carriers for Wireless Phase 1 and 2.
- ISO and Sarbanes Oxley auditor.

9-1-1 COMMUNICATIONS SUPERVISOR / TRAINER / EMD - ***Larimer County Sheriff*** 12/1994 – 10/2000

- All aspects of Emergency Call taking and Emergency dispatching law enforcement units, Quick Response Teams (QRT), air ambulances, dive teams, fire fighters, emergency services, Search and Rescue (SAR), SWAT.
- Communications Training Officer (CTO); Initial contact for complaints from the public, escalated and disciplined appropriately. Managed Emergency Medical Dispatch (EMD) program, EMD-QA, served on EMD committees.

<<PROPRIETARY OR CONFIDENTIAL INFORMATION INTENTIONALLY REMOVED>>

<<PROPRIETARY OR CONFIDENTIAL INFORMATION INTENTIONALLY REMOVED>>

Declaration Concerning Conflict of Interest and Confidential Information

Conflict of Interest:
I hereby certify that neither I, nor any member of my immediate family, nor any other party having influence over me, has a material, personal or financial relationship with any bidder, or to a direct competitor of any bidder under consideration by this proposal evaluation committee. I further certify that no other relationship, bias or ethical conflict exists which will prevent me from evaluating any proposal solely on its merits and in accordance with the Request for Proposal's evaluation criteria.

Furthermore, I agree to notify the Agency Project Leader and State Procurement Manager if my personal or financial relationship with one of the bidders is altered at any time during the evaluation process. If I am serving as the Project Leader of record, I agree to advise the State Procurement Manager and my supervisor of any change that could appear to represent a conflict of interest.

Confidential Information:
As an evaluation committee member, I may receive materials that have been determined to be confidential. I promise to keep these materials confidential and return all confidential material to the Agency Project Leader.

Third Party Contact:
I hereby certify that I will not engage in any contact or communication with any third party, including but not limited to any vendor, bidder, or potential bidder regarding this Request for Proposal or evaluation process. Further, if any such contact or communication should occur, or if I reasonably believe any such contact may have occurred or will occur, I will notify the Agency Project Leader and the State Procurement Manager immediately.

_____	_____
Date	Evaluation Committee Member
_____	_____
RFP Number	Print Name
	_____
	Agency/Department

STEPHEN F. O'CONOR, M.A., ENP *4768 Alamanda Drive • Melbourne, FL 32940 • 321-432-8159 (c) • 407-439-4911 (o) email: 911@cfl.rr.com*

OBJECTIVE Seeking a position as a Client Services Director or Manager

ABILITY SUMMARY

- Extensive knowledge and experience in Public Safety and the Criminal Justice System, with 10 years of management experience at the command staff level.
- Knowledge and experience in servicing customer accounts and providing the conduit between customers and the engineering and sales teams
- Highly effective communication skills
- Master of Arts in Criminal Justice, Rutgers University (+23 credits toward Ph.D.). Summa cum Laude graduate of Upsala College.
- FEMA ICS Courses completed; Professional Development Series courses in progress.

EMPLOYMENT

NGA 911, LLC. SEPT 2018-Present *Chief Compliance Officer*

- Technical Editor of the National Emergency Number Association's i3 Standard

SYNERGEM TECHNOLOGIES, INC. SEPT 2011-APRIL 2018 *1150 Revolution Mill Road – Studio 1 Greensboro, North Carolina Director of Client Services (40 hours/week)*

- Technical Editor of the National Emergency Number Association's i3 Standard fo for Next Generation 9-1-1 Candidate American National Standard (NENA-STA-010.3)

EDUCATION

MASTER OF ARTS 2000 ***Rutgers University School of Criminal Justice Newark, NJ*** Master's Essay: *Performance evaluation: A new paradigm* Served as teaching assistant to Dr. Ronald Clarke, University Professor, former Dean of the School of Criminal Justice and world-renowned criminologist in the field of crime prevention. BACHELOR OF SCIENCE 1989 ***Upsala College East Orange, NJ*** Summa Cum Laude. Majors: Public Safety Administration and Political Science

Mike DeWeese

mike.deweese@nga911.com

linkedin.com/in/mdeweese

Vice President of Technology | NG911 Technologist

Thought leader and senior executive team member known for deep technical knowledge. Holds a reputation in the industry for having a broad understanding of all elements of 9-1-1 from the data inception of call routing to call delivery for both legacy and Next Generation 9-1-1. Leverages extensive experience in countless projects and product developments; successfully contributed to or drove the development of 9-1-1 products and service delivery networks including A911 ESInet, AT&T ESInet, Viper 9-1-1 CPE along with Wireless and VOIP systems for call routing.

Core Competencies

Systems Architecture and Implementation Integration
9-1-1 Text Messaging Delivery Data Center Design and Implementation
Cloud Computing Vendor Management

Professional Experience

NGA 911, Beverly Hills, CA 4/2020 - Present
VP Technology 4/2020 - Present
Leading NextGen 911 technologies forward with a progressive company.

Intrado, Longmont, CO 3/2003 – 4/2020
VP Technology / Senior Technical Officer, 9/2009 – 4/2020
Utilized to lead the strategic direction of NG911 technology and products. Established collaboration and a common technical direction across business groups.

- Senior technologist for NG911 ESInet core elements and strategy.
- Senior member of executive staff influencing NG product and technical direction.
- Selected and guided implemented of TDM to SIP gateways with SS7 MGC.
- Provided guidance and expertise for NGCS core routing and bridging.
- Designed methodology and convinced major carrier and PSAP to replace DMS100 with TDM/IP gateways and NG CPE.
- Designed methodology and convinced major carrier to move legacy S/R's to ESInet routing.
- Negotiated and worked with major wireless carrier to interconnect and test full I3 PidfLo with ADR SIP bodies.
- Coinvented method to deliver alarm messaging to 9-1-1 centers via text.
- Devised methods to aggregate and deliver additional "relevant" data to PSAP's.
- Codesigned dedicated computing platform for NG 9-1-1 CPE.

Principal Systems Engineer, 3/2003 – 9/2009
Led or served as a key participant in various projects, initiatives and enhancements during a period of transition and growth for the company.

- Created the first IP network to deliver wireless Phase II location from a PDE.
- Deployed above network with PDE in a major carrier's market that enabled the first Wireless Phase II call with location.
- One of the core engineers listed on a patent for the first all IP call routing and data delivery system called IEN (Intrado Emergency Network), an early precursor to I3 with protocols still used for IP call delivery.
- Served as core engineer to enhance the aforementioned system that established the current
  Intrado A911 ESInet.

Principal Systems Engineer, continued

- Created and deployed the first ALI delivery IP network for 112 Texas PSAP's.
- Developed and deployed the first IP POI to terminate and deliver Vonage 9-1-1 calls in NYC.
- Engineered and deployed the first nationwide redundant VOIP POI network for 9-1-1 call routing and PSAP call delivery.

Additional Relevant Experience

Intrado Inc, Boulder, CO 1/1995 – 3/2003
Manager Networking Systems
Managed a network engineering staff for the creation and deployment of core supporting networks. Designed, built a managed Novell networks with support for core business applications. Built and managed first Intrado data center.

SCC Communications, Boulder, CO 4/1991 – 1/1995
Field Technician
Systems Engineer for development and integration of 9-1-1 local area and WAN networks. Installation and maintenance of PSAP CPE, CAD and RMS systems.

Competencies

- NENA I3 SIP flows and Data messaging
- SS7 and CAMA Telephony signaling and data systems in relation to supporting 9-1-1 systems.
- IP, BGP, SIP, VoIP, TDM, SS7, X.25, Sync and Async protocols and transport
- Cyber Security as applied to 9-1-1 CPE and ESInet

Candace Allred
P: (919) 280-8709 | **E:** candace.allred@nga911.com | **LI:** linkedin.com/in/candace-allred-02b08159

SUMMARY

20+ years relationship sales leadership experience within the public safety community. Executive leader with an extensive leadership experience delivering results across the globe through mission critical technologies. Passionate and enthusiastic professional with a proven record of fostering cultures that drive leadership effectiveness, employee engagement, customer satisfaction and business results.

SKILLS & EXPERTISE

· Strategic Sales & Business Development · Business Operations · Revenue Generation · Team Leadership · Staff Training & Development · Channel Development & Management · Outstanding People Skills · Excellent Communication Skills · Relationship Building · Project Management · Results Focused

---

EXPERIENCE

NGA 911 | Beverly Hills, CA | November 18, 2019 - Present

Vice President, Sales

Responsible for global sales and forecasting for NGA 911.

MICROAUTOMATION | Centreville, VA | January 7, 2019 – November 15, 2019

Vice President, Emergency Operations Solutions

Responsible for the total P&L for the Emergency Operations Solutions Practice within MicroAutomation. Including: Global Sales & Forecasting, Product Development & Innovation, Solutions Engineering & Architect, Proposal Management & Project Management, Channel Development & Management, Customer Training & Documentation.

FRONTIER COMMUNICATIONS | Stamford, CT | July 2011 – Dec 31, 2018

Director, National Public Safety

Responsible for the total P&L for the Public Safety team within Frontier Communications. Including: National Sales & Forecasting, Project Management, Solutions Sales Engineering, Channel Management & Product Portfolio.

VERIZON | Durham, NC | February 28, 1998 – July 2011

9-1-1 Product Manager, 9-1-1 Service Manager Specialist, 9-1-1 Senior Project Manager, 9-1-1 SME Business Development:

Responsible for the total P&L for the Public Safety team within Verizon. Including: National Public Safety / 9-1-1 Product Management, National 24x7x365 Public Safety / 9-1-1 Service Manager Specialist, National Public Safety / 9-1-1 Senior Project Manager, National 9-1-1 Sales (Subject Matter Expert in Business Development).

ACHIEVEMENTS

Top Sales Leadership & Presidents Club Award

Top Sales & Presidents Award

MEMBERSHIPS

National Emergency Number Association (NENA)

Association of Public-Safety Communications Officials (APCO)

NGA 911 Employee	Ref #1 Name	Ref #2 Name	Ref #3 Name
Anne DeGraff, PMP	Greg Crawford, ez911	Whitney Butler, Miller-Bake County, GA	Janet Boland, Ashtabula County, OH
Michelle Bland, ENP	Dee Dee Teel, California Highway Patrol	Ella Sotello	Katie Sanborn
Roger Nicholls	William Bordeaux Long Beach Pd	Brian Flinn Downey Police	Jack Armstrong Frontier Communications
Shelly Guenther, ENP	Sharon Counterman, Winbourne Consulting	Steve Marzolf, Retired State of Virginia	Ken Tweedy, WestTel Communications
Mark LeMonn	Bill Shaw, California Highway Patrol	Dee Dee Teel, California Highway Patrol	Jeff Visgor, VPI Inc
Ed Vea	John Stevens - New Hamsphire FirstNet SPOC	Ken Tweedy, WestTel Communications	Micheal Inserra, Samsung Federal/DOD
Miguel Martinez	Ron Dunn - Santa Barbara PD, CA	Carl Simpson - El Paso Teller, CO	Justin Grenier - St George, UT
Steve O'Conor	Brandon Abley, NENA	Pete Eggimann, Metropolitian Emergency Services Board	Jim Shepard, 911 Datamster
Candace Allred	Renee Hardwick, Horry County 911 SC	Dave Hopkins, Steuben County 911 NY	Sandra Dyre, Arizona
Mike DeWeese	Stephen Meer, Ande Inc	John Snapp, Intrado	Mike Pappas, Orban Labs

Please address the information to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

2.1 Acronyms/Abbreviations

Acronyms/abbreviations used in this document have been included in the original standard document 75-001.

3 Operations or Technical Description

The following instructions and clarifications are provided to guide the auditor.

- For each section, provide the auditor name, title, and contact information, as well as the date the audit section was completed
- For each audit question, choose C for "comply," No for "does not comply" or not applicable (N/A) for "the requirement is not applicable." If N/A is chosen, provide commentary as to why the question isn't application in the comments column. Items marked No are deemed out of compliance with the NG-SEC standard.
- Please refer to the NG-SEC standard (NENA Document 75-001) itself as a reference for questions of interpretation.
- As noted earlier, audit questions consist of Requirements (R) and Best Practices (BP).
- For questions or sections not audited please indicate they were not audited using the comments column

One Nation 9-1-1 One Number

Section 1 - Senior Management Statement

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
1	4.1	Has Senior Management created a Senior Management Statement (SMS) of Policy? (Audit Guidance: this could take the shape of a security plan, executive level security policy, or other such documents. The auditor should use his/her discretion as to whether the document in question meets the requirements of this portion of the NG-SEC standard)	R	■ C ☐ No ☐ N/A	
2	4.1	Does the SMS designate the person responsible for security (e.g. Security Administrator)?	R	■ C ☐ No ☐ N/A	
3	4.1	Does the SMS clearly document the security goals and objectives of the organization?	R	■ C ☐ No ☐ N/A	

Section 1 - Senior Management Statement Auditor: Ed Vea Date: 1/15/2019 _____

One Nation 9-1-1 One Number

Section 2 - Acceptable Use Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
4	4.2	Does the organization have an Acceptable Usage Policy?	R	■ C ☐ No ☐ N/A	
5	6.6	Are any and all actual, attempted, and/or suspected misuses of Public Safety assets reported and documented by appropriate organizations?	R	■ C ☐ No ☐ N/A	

Section 2 - Acceptable Use Policy Auditor: Ed Vea Date: 1/15/2019 _____

One Nation 9-1-1 One Number

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
6	4.2	Does the organization have an Authentication / Password Policy?	R	☐ C ☐ No ☐ N/A	
7	7.1.1	Is each individual requiring access to the NG9-1-1 System provided a unique Identification and authentication?	R	☐ C ☐ No ☐ N/A	
8	7.1.1	Do individuals share their authentication information (including usernames and passwords) with other individuals or groups?	R	☐ C ☐ No ☐ N/A	
9	7.1.2	Are requests for new User Accounts, User IDs, and File and Resource authorization documented? (Audit Guidance: review applicable documentation and processes for adequacy of process and adherence to process)	R	☐ C ☐ No ☐ N/A	
10	7.1.2	Do personnel performing entity or security administration ensure that only approved entities are granted access?	R	☐ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
11	7.1.2.1	Does the organization have procedures for changing access authority?	R	■ C ☐ No ☐ N/A	
12	7.1.2.1	Does the organization have procedures for removing access authority for terminated personnel?	R	■ C ☐ No ☐ N/A	
13	7.1.3	When system to system access is implemented does the system mask individual accountability for transactions? (Audit Guidance: The system shall not mask individual accountability for transactions)	R	■ C ☐ No ☐ N/A	
14	7.1.3	When system to system access is implemented is the source system authenticated before each transfer session?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
15	7.1.3	When system to system access is implemented and push technology is utilized, is the destination authenticated by the source?	R	■ C ☐ No ☐ N/A	
16	7.1.3	When system to system access is implemented and a continuous connection is utilized, was authentication performed at the initial connection?	R	■ C ☐ No ☐ N/A	
17	7.1.3	When system to system access is implemented are individuals accessing any of the systems required to Authenticate when initially accessing each system?	R	■ C ☐ No ☐ N/A	
18	7.1.5	Are Authentication Credentials displayed in an obscured format when entered on computer screens? (Auditor Guidance: Check to see if passwords can be seen on the screen when typed in. They should not be able to be seen so as to prevent "shoulder surfing.")	R	■ C ☐ No ☐ N/A	
19	7.1.4	Are users locked out after no more than 5 invalid sign on attempts?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
20	7.1.5	Are Default and Null Passwords changed when installing new equipment or software?	R	☐ C ☐ No ☐ N/A	
21	7.1.5	Are Authentication Credentials encrypted when stored on a computer?	R	☐ C ☐ No ☐ N/A	
22	7.1.5	When two-factor authentication is used, (e.g. SecurID + Pin or Certificate + Passphrase) are two authentication factors stored in such fashion that one incident can compromise both? (Auditor Guidance: e.g. password or pin isn't written down on the token, or stored with the token)	R	☐ C ☐ No ☐ N/A	
23	7.1.5.1	All user accounts shall require a password	R	☐ C ☐ No ☐ N/A	
24	7.1.5.1	Passwords are not based on the user's account name.	R	☐ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
25	7.1.5.1	Passwords must meet the following complexity requirements: • Contains characters from three of the following four categories: ○ Uppercase alphabet characters (A–Z) ○ Lowercase alphabet characters (a–z) ○ Arabic numerals (0–9) ○ Non-alphanumeric characters (for example, !$#,%)	R	■ C ☐ No ☐ N/A	
26	7.1.5.1	Minimum password length shall be 8 characters or greater	R	■ C ☐ No ☐ N/A	
27	7.1.5.1	Minimum password age shall be 3 days or greater	R	■ C ☐ No ☐ N/A	
28	7.1.5.1	Maximum password age **requirement** 60 days or less	R	☐ C ☐ No ■ N/A	]Maximum password age is 45 days.

One Nation 9-1-1 One Number

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
29	7.1.5.1	Maximum password age **recommendation** 30 days	BP	☐ C ☐ No ☐ N/A	
30	7.1.5.1	If feasible, authentication schemes shall provide for password exchange in a format that cannot be captured and reused/replayed by unauthorized users to gain authenticated access, e.g., random password generating tokens or one-way encryption (also known as hashing) algorithms.	R	☐ C ☐ No ☐ N/A	
31	7.1.5.1	When using temporary passwords they shall be required to be changed upon initial login	R	☐ C ☐ No ☐ N/A	
32	7.1.5.1	Passwords should not be hard coded into automatic login sequences, scripts, source code and batch files, etc., unless required by business need and then only if protected by security software and/or physical locks on the workstation, and passwords are encrypted.	BP	☐ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
33	7.1.5.1	Password construction should be complex enough to avoid use of passwords that are easily guessed, or otherwise left vulnerable to cracking or attack. Names, dictionary words, or combinations of words shall not be used; nor shall they contain substitutions of numbers for letters, e.g., s3cur1ty. Repeating numbers or sequential numbers shall also not be used	BP	☐ C ☐ No ☐ N/A	
34	7.1.5.1	Passwords should not contain sequences of three (3) or more characters from the user's login ID or the system name.	BP	☐ C ☐ No ☐ N/A	
35	7.1.5.1.4	Passwords should not contain sequences of three (3) or more characters from previous chosen or given passwords.	BP	☒ C ☐ No ☐ N/A	
36	7.1.5.1.5	Passwords should not contain a sequence of two (2) or more characters more than once, e.g., a12x12.	BP	☒ C ☐ No ☐ N/A	
37	7.1.5.1.5	Passwords used to access Public Safety systems and resources should not be used on any external systems, e.g., Home PC's, Internet sites, shared public systems.	BP	☒ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
38	7.1.5.2	When Passphrases are used do they have a required length of at least 15 characters? (Audit Guidance: Alpha, numeric and special characters may all be used.)	R	■ C ☐ No ☐ N/A	
39	7.1.5.2	When Passphrases are used they shall not use repeating words, or sequential characters or numbers.	R	■ C ☐ No ☐ N/A	
40	7.1.5.2	When Passphrases are used they shall be case sensitive		■ C ☐ No ☐ N/A	
41	7.1.5.2	When Passphrases are used and where they are automatically set or set by administrator, the initial passphrase shall be randomly generated and securely distributed.	R	■ C ☐ No ☐ N/A	
42	7.1.5.2	When Passphrases are used first-time users may create their own passphrase after authenticating.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
43	7.1.5.2	When Passphrases are used Users shall have the capability of changing their own passphrase online. However, the old passphrase shall be correctly entered before a change is allowed	R	■ C ☐ No ☐ N/A	
44	7.1.5.2	When Passphrases are used a lost or forgotten passphrase can be reset only after verifying the identity of the user (or process owner) requesting a reset.	R	■ C ☐ No ☐ N/A	
45	7.1.5.2	When Passphrases are used passphrases shall automatically expire every 180 days or less for General Users.	R	■ C ☐ No ☐ N/A	
46	7.1.5.2	When Passphrases are used systems shall notify users at expiration time and allow the user to update the passphrase.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
47	7.1.5.2	When Passphrases are used and when it is changed, the old passphrase shall not be reused until either: 1. at least four (4) other passphrases have been used, or 2. at least 4 months have passed.	R	■ C ☐ No ☐ N/A	
48	7.1.5.2	When Passphrases are used systems shall not display the passphrase in clear text as the user enters it.	R	■ C ☐ No ☐ N/A	
49	7.1.5.2	When Passphrases are used shall not be stored in script files or function keys.	R	■ C ☐ No ☐ N/A	
50	7.1.5.2	When Passphrases are used Passphrases shall always be encrypted for transmission	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
51	7.1.5.3	If Digital Certificates are used is a revocation procedure in place if compromised?	R	☐ C ☐ No ☐ N/A	
52	7.1.5.3	Are Digital Certificates kept current and expired or invalid certificates not used?	R	☐ C ☐ No ☐ N/A	
53	7.1.5.3	Cryptographic implementations use standard implementations of security applications, protocols, and format?	R	☐ C ☐ No ☐ N/A	
54	7.1.5.3	Cryptographic implementations shall be purchased from reputable vendors?	R	☐ C ☐ No ☐ N/A	
55	7.1.5.3	If Cryptographic solutions are developed in-house staff should be properly trained in cryptology.	R	☐ C ☐ No ☐ N/A	
56	7.1.5.3	Do employees protect and safeguard any encryption keys for which they are responsible?	R	☐ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
57	7.1.5.3	Employees do not share private encryption keys with others except when applicable or appropriate authorities demand the key be surrendered (Termination, Promotion, Investigation etc.)	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
58	7.1.5.3	A process exists by which current validity of a certificate can be checked and a certificate can be revoked Validity testing includes: • Do key holders initiate key revocation when they believe access to their keys have been compromised • Has the Certificate Authority signature on the certificate been validated • Is the date the certificate is being used within the validity period for the certificate • The Certificate Revocation List for the certificates of that type are checked to ensure they have not been revoked • The identity represented by the certificate - the "distinguished name" is valid (distinguished name refers to the location in the x.500 database where the object in question exists)	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
59	7.2.6	In order to help assure segregation of duties, developers shall not be System Administrators for the Production Systems they have developed (small, stand-alone systems can be excepted from this requirement)	R	■ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy Auditor: Ed Vea Date: 1/15/2019 _____

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
60	4.2	Does the organization have a Data Protection Policy?	R	■ C ☐ No ☐ N/A	
61	6.2	Application, system, and network administrators perform a security self-review on systems for which they have operational responsibility at least once per year.	R	■ C ☐ No ☐ N/A	
62	6.2	The self-review assessments are in writing and retained by the Security Manager and the NG9-1-1 Entity	R	■ C ☐ No ☐ N/A	
63	6.2	A copy of the current security self-review or security assessments/audit reports are retained until superseded by another security assessment or the system is retired	R	■ C ☐ No ☐ N/A	
64	6.3	Application, system, and network administrators have identified which security solutions have or require periodic review and the frequency by which they shall occur (Auditor Guidance: This finding refers to recurring security solutions, such as audit logs, or Intrusion Prevention Systems.)	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
65	6.3	Application, system, and network administrators conduct the periodic reviews defined in audit number 64	R	■ C ☐ No ☐ N/A	
66	6.4.2	All networks have a clearly defined purpose or mission so appropriate security measures can be implemented. (Auditor Guidance: To verify if this has occurred request documentation such as drawings, mission statements, policies, etc., that clearly indicate that the network in question's mission is defined)	BP	■ C ☐ No ☐ N/A	
67	6.4.3	For systems on the network in question, an accurate and current inventory is maintained. (Auditor Guidance: Request copies of a current inventory. Acceptable inventories included automated systems, paper logs, or logbooks).	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
68	6.4.3	Inventories are appropriately classified and in accordance with the implemented information classification and protection policy	R	■ C ☐ No ☐ N/A	
69	6.4.4	All administrative access to the network is precisely controlled with appropriate identification, authentication, and logging capabilities	R	■ C ☐ No ☐ N/A	
70	6.4.4	Uncontrolled points of entry are not allowed on the network	R	■ C ☐ No ☐ N/A	
71	6.4.4	All point of ingress and egress to a network are fully documented, approved, and protected	R	■ C ☐ No ☐ N/A	
72	6.4.5	Connecting multi-homed computers to networks that have different security postures is not allowed	R	■ C ☐ No ☐ N/A	
73	6.4.5	When multi-homed computers are implemented Host IPS shall be installed on the multi-homed computer	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
74	6.4.5	When multi-homed computers are implemented, all other appropriate security countermeasures, including those described in this document are implemented on multi-homed computer	R	■ C ☐ No ☐ N/A	
75	6.4.5	When multi-homed computers are implemented Anti-virus is running on both/all networks and the multi-homed computer	R	■ C ☐ No ☐ N/A	
76	6.4.5	When multi-homed computers are implemented, IP-forwarding is explicitly disabled?	R	■ C ☐ No ☐ N/A	
77	6.4.5	When multi-homed computers are implemented multi-homed computers should have 'Hardened Operating Systems'	BP	■ C ☐ No ☐ N/A	
78	6.4.5	When multi-homed computers are implemented multi-homed computers should have 'Hardened Applications'	BP	■ C ☐ No ☐ N/A	
79	6.4.6.3	Firewalls are maintained at all 4.9GHz network boundaries	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
80	7.1.2.2	Does the organization have procedures for reviewing access authority for inactive accounts?	R	■ C ☐ No ☐ N/A	
81	7.2.1	Accounts shall be created based on "Least Privilege"	R	■ C ☐ No ☐ N/A	
82	7.2.1	Are users given access to only the functions and data necessary to perform their assigned duties	R	■ C ☐ No ☐ N/A	
83	7.2.1	All computer resource access is restricted to only the command, data, and systems necessary to perform authorized functions	R	■ C ☐ No ☐ N/A	
84	7.2.1.1	All data has appropriate minimum access privileges, e.g. read, write, modify, as defined by the data owner and is in compliance with local laws	R	■ C ☐ No ☐ N/A	
85	7.2.1.2	Access is restricted to only those individuals and groups with a business need, and subject to the data's classification.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
86	7.2.1.2	Unrestricted/global access should be avoided whenever possible and is only used where specifically appropriate and with the data owners approval	BP	■ C ☐ No ☐ N/A	
87	7.2.1.2.a	Is an annual review of all resources, (e.g., files or directories, to which access is not restricted, i.e., have universal or public access) shall be performed and the resource owners shall be notified of the results.	R	■ C ☐ No ☐ N/A	
88	7.2.1.2.b	Is group membership restricted only to persons performing the given function?	R	■ C ☐ No ☐ N/A	
89	7.2.1.3	All unnecessary services and network services are disabled.	R	■ C ☐ No ☐ N/A	
90	7.2.1.3	Any application service which lets the user escape to a shell, provide access to critical system files, or maps/promotes IDs to privileged user levels is disabled	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
91	7.2.1.3a	Is an annual review for compliance with Audit Area 90 completed and findings documented?	R	■ C ☐ No ☐ N/A	
92	7.2.1.3a	Are findings from the audit conducted in Audit Area 92 closed or has the risk been managed?	R	■ C ☐ No ☐ N/A	
93	7.2.1.4	Administrator shall ensure that system access controls (e.g. filters that restrict access from only authorized source systems), are used where they exist and only contain necessary system authorizations?	R	■ C ☐ No ☐ N/A	
94	7.2.1.4.a	Is an annual review for compliance with Audit Area 93 completed and findings documented?	R	■ C ☐ No ☐ N/A	
95	7.2.1.4.a	Are findings from the audit conducted in Audit Area 94 closed or has the risk been managed?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
96	7.2.1.5	Do Administrators use non-Administrative accounts when performing non-Administrative tasks? (Auditor Guidance: The Administrator should maintain two user accounts. One with Administrator / privileged rights and one without. When performing administrative functions they should use their Administrator account. When not performing such tasks they use a "normal" user-level account. The use of "runas" or "superuser" features is allowable).	R	■ C ☐ No ☐ N/A	
97	7.2.1.6	Do ALL System Administrators have a personal Administrator account rather than use a generic account? (Auditor Guidance: Administrators shall not use default, or built-in Administrator accounts except during disaster recovery or initial installations. Each Administrator must have his or her own unique Administrator account to provide traceability. Administrator accounts shall never be shared)	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
98	7.2.1.6	Systems that do not support unique administrative accounts should not be used as they pose a significant threat. Entities are encouraged to prevent inclusion of such systems onto the NG9-1-1 networks. .	BP	■ C ☐ No ☐ N/A	
99	7.2.2	The login "Warning Notice" is displayed during the boot up or logon sequence (either before or after the authentication, preferably before, but it is displayed before any substantive data	R	■ C ☐ No ☐ N/A	
100	7.2.2	The "Warning Notice" remains displayed until positive action by the user is taken to acknowledge the message	R	■ C ☐ No ☐ N/A	
101	7.2.3	Computer resources, systems, applications, and networks shall be restricted at all times to authorized personnel	R	■ C ☐ No ☐ N/A	
102	7.2.3	Where possible access control is accomplished with "role bases" privileges that assign users to roles and grant access to members of a role rather than to individuals	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
103	7.2.4	Non-privileged users do not have read/write access to system files or resources such as protected memory, critical devices, executable programs, network configuration data, application file systems, etc.	R	■ C ☐ No ☐ N/A	
104	7.2.4	Only administrative users are assigned passwords to access and modify sensitive files/resources	R	■ C ☐ No ☐ N/A	
105	7.2.5	Files/File Folders are restricted to only those requiring access	R	■ C ☐ No ☐ N/A	
106	7.2.5	Rights assigned only to those who actually need them and are documented as needing them	R	■ C ☐ No ☐ N/A	
107	7.2.5	Access Groups used whenever possible to simplify administration	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
108	7.2.5	Has the organization renamed built-in Administrator accounts?	R	■ C ☐ No ☐ N/A	
109	7.2.5	Anonymous and/or guest accounts are disabled to prevent exploitation	R	■ C ☐ No ☐ N/A	
110	7.2.5	Are periodic audits of user account access conducted to ensure users have only the "effective rights" required to perform their functions?	R	■ C ☐ No ☐ N/A	
111	7.2.6	Are Production and Non-Production systems separated to protect integrity of the Production System?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
112	7.2.6	If the Non-Production System is intended to become a Production System is it governed by the requirements of a Production System (Auditor Guidance: While it is unlikely a non-production system will be "in-scope" during an audit, if it is, this requirement refers to the need for that system to comply with all requirements herein)	R	■ C ☐ No ☐ N/A	
113	7.2.6	Production data is not copied off the system without the service owner's permission and is protected to an equivalent or greater degree	R	■ C ☐ No ☐ N/A	
114	7.2.6	Production systems do not contain any software development tools except where essential for the application	R	■ C ☐ No ☐ N/A	
115	7.2.6	While software development tools may be installed for software upgrades, or installation of new software packages, or for troubleshooting, but they must be removed immediately after use	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
116	7.2.6	When software development tools are essential for production operation, they must be inaccessible to users	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
117	7.2.7	All devices capable of enforcing a password protected screensaver or a keyboard lock do so with an inactivity timeout of 15 minutes or less exceptions will comply with Para 7.2.7.1, .2,and .3 The following are exceptions: • When superseded by local public safety policy • Users in a customer facing role, such as sales representatives making sales presentations, may have the automated screensaver temporarily disabled so long as the following conditions are met: a. The automated screensaver shall not be deactivated for any longer than justified and not for a period greater than four hours b. While the automated screensaver is deactivated the screensaver shall be manually activated whenever the device is to be left unattended, even for a brief period of time • Devices that are dedicated to displaying messages/information to a number of people, for example, in a reception area or in an operations center, may have their screensaver disabled so long as the following conditions are met: a. Access (physically and logically) to the device, including its keyboard and user IDs, is controlled in accordance with all applicable physical and logical security requirements b. Visibility of the display is restricted to only individuals authorized to see the data that will be displayed	R	☐ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
118	7.2.7	All devices not capable of enforcing a password protected screensaver or a keyboard lock will have controlled access in accordance with all applicable physical and logistical security or have session inactivity timeouts set for 15 minutes	R	■ C ☐ No ☐ N/A	
119	7.2.7	Consoles not capable of enforcing a password protected screensaver or a keyboard lock are configured to automatically log out after 15 minutes of inactivity	R	■ C ☐ No ☐ N/A	
120	7.2.7	If automatic inactivity logout is not supported are users required to logout when console is left unattended	R	■ C ☐ No ☐ N/A	
121	7.2.8.4	Peer to Peer Networking is NOT allowed in the NG 9-1-1 environment	R	■ C ☐ No ☐ N/A	
122	7.3.1	NG9-1-1 Entity information which is either discoverable or otherwise requested by the general public or media must be clearly identified.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
123	7.3.1	Specific guidelines must be written and followed to document what data is released, when and to whom when releasing NG9-1-1 Entity information which is either discoverable or otherwise requested by the general public or media must be clearly identified.	R	■ C ☐ No ☐ N/A	
124	7.3.1	The guidelines identified in Audit Area 123 shall capture any specific release requirements for data such as video, names, call content, message text, or other personal content	R	■ C ☐ No ☐ N/A	
125	7.3.1	Where such data is intermingled with other data of differing classification, consideration shall be given to replicating the public domain data into a separate data store	BP	☐ C ☐ No ■ N/A	No public domain data.
126	7.3.2	Where email is used to send NG 9-1-1 Sensitive Information, is the message clearly marked with its classification, do the senders ensure recipients are aware of the safeguards required.	R	■ C ☐ No ☐ N/A	
127	7.3.2	Where email is used for emergency communications, senders must verify the recipient's email ID is correct prior to sending	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
128	7.3.2	Where email is used for emergency communications, the recipient shall understand the safeguards associated with the proprietary marking	R	■ C ☐ No ☐ N/A	
129	7.3.2	Where email is used for emergency communications and email with Sensitive Information is printed it shall be protected according to the rules associated with its classification	R	■ C ☐ No ☐ N/A	
130	7.3.2	Where email is used for emergency communications, Sensitive Information must be encrypted when sent by email	R	■ C ☐ No ☐ N/A	
131	7.3.2	Does the NG9-1-1 entity control the domain used for email communication unless otherwise covered by a formal contractual document (Auditor Guidance: The intent of this audit question is to ensure that entities register a legitimate DNS domain name for any NG9-1-1 communication as opposed to using free email services, etc.).	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
132	7.3.2	Internal NG9-1-1 Entity email should not be made available on a 9-1-1 call-taking position workstation, but rather on a separate system.	BP	☐ C ☐ No ■ N/A	Not involved in call-taking positions.
133	7.3.2	In lieu of detailed security standards for email use in an NG9-1-1 environment, NG9-1-1 Entities are encouraged to follow best practices such as those offered by the National Institute for Standards and Technology (NIST)	BP	■ C ☐ No ☐ N/A	
134	7.3.2.1	Individual messaging services have been evaluated to ensure they comply with NG9-1-1 Entity production and security requirements	R	■ C ☐ No ☐ N/A	
135	7.3.3.1	Do cryptographic installations use industry standard cryptographic algorithms and standard modes of operations and comply with the laws of the United States	R	■ C ☐ No ☐ N/A	
136	7.3.3.1	The use of encryption algorithm or device complies with the laws of the United States and any country in which there are plans to use data encryption	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
137	7.3.3.1	It is recommended the algorithm certified by the NIST FIPS 140 certification, currently AES, be used	BP	■ C ☐ No ☐ N/A	
138	7.3.3.1	Where there are no US federal standards for specific encryption functions e.g. public key cryptography, message digests, commercial algorithms may be used.	BP	☐ C ☐ No ■ N/A	Federal standards are used.
139	7.3.3.1	Implementations of cryptography shall follow best commercial practices e.g. Public Key Cryptography Standards.	R	■ C ☐ No ☐ N/A	
140	7.3.3.1	Implementations and modes shall use the strongest available product	R	■ C ☐ No ☐ N/A	
141	7.3.3.2	If Public Key Cryptography is used does the NG9-1-1 entity have a Public Key Infrastructure to manage and distribute public keys?	R	■ C ☐ No ☐ N/A	
142	7.3.3.2	Does the PKI manage both Symmetric and Asymmetric Keys through the entire life cycle?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
143	7.3.3.2	Encryption Devices and any server used to store encryption keys are protected from unauthorized access	R	☐ C ☐ No ☐ N/A	
144	7.3.3.2	Key generation is performed using a commercial tool that comply with x.509 standards and produce x.509 compliant keys.	R	☐ C ☐ No ☐ N/A	
145	7.3.3.2	Keys are not generated using predictable function or values	R	☐ C ☐ No ☐ N/A	
146	7.3.3.2	Symmetric keys must be at least 112 bits in length and Asymmetric keys at least 1024 bits in length	R	☐ C ☐ No ☐ N/A	
147	7.3.3.2	Keys are distributed to appropriate recipients through secure channels	R	☐ C ☐ No ☐ N/A	
148	7.3.3.2	Keys used to secure stored data are safeguarded so authorized persons can recover them at any time	R	☐ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
149	7.3.3.3	Does the Public Key Infrastructure (PKI) have a documented Certificate Practice Statement defining how security is provided for the infrastructure, registration process, relative strength of the system, and Legitimate uses?	R	■ C ☐ No ☐ N/A	
150	7.3.3.3	Does the PKI implement a registration process that identifies the requester by an acceptable form of identification before the Certificate Authority (CA) creates a Digital Certificate?	R	■ C ☐ No ☐ N/A	
151	7.3.3.3	Does the PKI have a review process for validity checks and revocation as required?	R	■ C ☐ No ☐ N/A	
152	7.3.3.3	Do key holders initiate key revocation if they believe access to their keys have been compromised?	R	■ C ☐ No ☐ N/A	
153	7.4.1	Are all files and software scanned for viruses and malicious code, and verified as free of logic bombs or other malicious code?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
154	7.4.3	Does the NG 9-1-1 entity use licensed industry standard antivirus (or anti-malware) software on all devices capable of running it?	R	■ C ☐ No ☐ N/A	
155	7.4.3	Does the NG 9-1-1 entity, install and maintain the latest version (including engine) of their licensed anti-virus software?	R	■ C ☐ No ☐ N/A	
156	7.4.3	Is the antivirus software installed and maintained on any personal equipment used for business functions?	R	■ C ☐ No ☐ N/A	
157	7.4.3	Is the software current with the latest available and applicable virus definitions?	R	■ C ☐ No ☐ N/A	
158	7.4.3	Does the software scan all files when opened and/or executed (including files on network shares)?	R	■ C ☐ No ☐ N/A	
159	7.4.3	Does the software scan files on local drives at least once a week?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
160	7.4.3	Does the software scan all files, attachments, and software received via email and/or downloaded from websites before opening?	R	■ C ☐ No ☐ N/A	
161	7.4.3	Does the software scan all removable media and software (including new workstations equipped with pre-loaded software) before opening and/or executing?	R	■ C ☐ No ☐ N/A	
162	7.4.3	Does the NG 9-1-1 Entity scan all removable media and software before opening and/or executing if it has not been kept secure within its control?	R	■ C ☐ No ☐ N/A	
163	7.4.3	Are all files made available as network shares scanned at least once per week?	R	■ C ☐ No ☐ N/A	
164	7.5.4	Does the NG 9-1-1 Entity have a backup procedure?	R	■ C ☐ No ☐ N/A	
165	7.5.4	Is a copy of the routine full backup media described in Audit Area 164 sent to a secure offsite location?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
166	7.6	All systems, applications, and databases have internal controls for logging, tracking, and personnel accountability	R	☐ C ☐ No ☐ N/A	
167	7.6.1	All systems, including but not limited to applications and databases, have a security event record(log) capable for after-the-fact investigation of loss, impropriety, or other inappropriate activity	R	☐ C ☐ No ☐ N/A	
168	7.6.2	A written Security Audit Log Review Plan has been developed	R	☐ C ☐ No ☐ N/A	
169	7.6.3	A Security Alarm Plan has been developed and documented which sets criteria for generating alarms, who is notified, and what actions are to be taken.	R	☐ C ☐ No ☐ N/A	
170	8.3	Sensitive data is printed only on attended printers or on printers in a secured area. Distribution is controlled and printouts of sensitive information are secured when not in use.	R	☐ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
171	8.3	Data stored on removable media that are external to the system hardware is safeguarded.	R	■ C ☐ No ☐ N/A	
172	8.3	Personal storage devices are not used within the NG9-1-1 entity location. (Auditor Guidance: Examples of personal storage devices include USB Thumbstick, etc.)	R	■ C ☐ No ☐ N/A	
173	8.3	When storage media and output is destroyed it is in a manner that contents cannot be recovered or recreated	R	■ C ☐ No ☐ N/A	
174	8.3	When producing copies containing classified, the originals and copies are not left unattended	R	■ C ☐ No ☐ N/A	
175	8.3	NG9-1-1 Entity personnel ensure re-used storage media is "clean" (i.e. does not contain any residual of information from previous uses)	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
176	8.3	All media distributed outside NG9-1-1 Entity is either new or comes directly from a recognized pool of "Clean" media	R	■ C ☐ No ☐ N/A	
177	8.4.2	If possible, information resources using a power supply are connected to electrical outlets and communications connections that utilize surge protection	BP	■ C ☐ No ☐ N/A	
178	8.6.2.10	Combustible materials are not stored in the computer center or server room	R	■ C ☐ No ☐ N/A	
179	8.6.2.11	Furniture, storage cabinets, and carpets are of nonflammable material.	R	■ C ☐ No ☐ N/A	
180	8.6.2.12	Carpets are anti-static.	R	■ C ☐ No ☐ N/A	
181	8.6.2.6	All critical information resources are on UPS	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
182	8.6.2.7&.8	Food, drinks, or smoking is not allowed in the server room	R	■ C ☐ No ☐ N/A	
183	8.6.2.9	Storage under raised floors or suspended ceilings is prohibited.	R	■ C ☐ No ☐ N/A	

Section 4 – Data Protection Auditor: Ed Vea Date: 1/15/2019 _____

One Nation 9-1-1 One Number

Section 5 - Exception Request / Risk Assessment

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
184	12	An Exception Approval / Risk Assessment process is in place.	R	■ C ☐ No ☐ N/A	
185	12	The exception approval and risk acceptance process includes Risk Justification, Risk Identification, Risk Assessment, Risk analysis, and Risk Acceptance and Approval.	R	■ C ☐ No ☐ N/A	
186	12	The exception approval and risk acceptance process is documented on each Exception Approval / Risk Acceptance Form (EA/RAF), including the names and contact information of the people who carried out the analysis.	R	■ C ☐ No ☐ N/A	
187	12.1	The EA/RAF process is followed for "ALL RISKS" (e.g., security vulnerabilities cannot be fixed or security patched, or cases of non-compliance with this Security Standard.	R	■ C ☐ No ☐ N/A	
188	12.1	The specific non-compliance or vulnerability documented in each EA/RAF was reviewed by NG9-1-1 Entity security organization and the legal department.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 5 - Exception Request / Risk Assessment

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
189	12.1	The actual form is maintained and tracked by the NG9-1-1 Entity Security Risk Manager, the Security Point of Contact, and all involved parties.	R	■ C ☐ No ☐ N/A	
190	12.2.1	The NG9-1-1 Entity has assigned a Security Risk Manager to manage security risks and is responsible for completing the EA/RAF in a complete and accurate manner prior to submitting to the Security Point of Contact / Team for review.	R	■ C ☐ No ☐ N/A	
191	12.2.1	The Security Risk Manager collaborates with other members of the pertinent security team in completing the form and obtains the approval signature from the NG9-1- Entity Risk Acceptance Approver.	R	■ C ☐ No ☐ N/A	
192	12.2.1	The Security Risk Manager is an employee or an authorized agent acting on behalf of the NG9-1-1 Entity.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 5 - Exception Request / Risk Assessment

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
193	12.2.1	The Security Risk Manager is the person identifying the need for the execution of the exception approval and risk acceptance process with technical and business knowledge of the asset(s) at risk or, meets 195	R	■ C ☐ No ☐ N/A	
194	12.2.1	The Security Risk Manager is a system administrator, systems engineer, project manager, or other key stakeholder with technical and business knowledge of the asset(s) at risk.	R	■ C ☐ No ☐ N/A	
195	12.2.1	The Security Risk Manager acts as Point of Contact for the organization owning the identified asset(s) at risk within the scope of the exception approval and risk assessment process for the duration of the EA/RAF	R	■ C ☐ No ☐ N/A	
196	12.2.1	If the Security Risk Manager leaves the entity or is changes job during the active duration of the EA/RAF, a new Security Risk Manager is identified to fill the role	R	■ C ☐ No ☐ N/A	
197	12.2.2	A Security Point of Contact / Team is assigned to review for completeness, accuracy, and consistency and subject matter expertise.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 5 - Exception Request / Risk Assessment

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
198	12.2.2	For high level risks, a team of Subject Matter Experts (SME) is assembled to review, document concurrence, and sign the EA /RAF prior to submission for final approval.	R	☐ C ☐ No ☐ N/A	
199	12.2.3	Has the senior official of the NG9-1-1 Entity has signed forms accepting complete accountability for any identified risk?	R	☐ C ☐ No ☐ N/A	
200	12.3	Risks to the NG9-1-1 Entity are acknowledged, assessed, and managed according to their severity.	R	☐ C ☐ No ☐ N/A	
201	12.3	Responsibility is not delegated to subordinates or peers, and adheres to the management level or higher.	R	☐ C ☐ No ☐ N/A	
202	12.3	The Risk Acceptance Approver is the senior manager with financial and legal responsibilities for the services and operation of the specific NG9-1-1 Entity.	R	☐ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 5 - Exception Request / Risk Assessment

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
203	12.3.1	The NG9-1-1 entity manages the process flow as noted below: 1. The NG9-1-1 Entity's Security Risk Manager identifies, justifies, assesses, and analyzes the risk. If the identification and/or analysis of the risk prove to be difficult, then a security team shall be contacted for assistance. The Security Risk Manager shall complete the EA/RAF, including Risk Justification, identifying the Security POC / Team, and NG9-1-1 Entity Risk Acceptance Approver. 2. The Security Point of Contact / Team shall assign the EA/RAF a globally unique tracking identifier / document number, review the form, determine or agree to who the NG9-1-1 Entity senior management approver is, discuss with Security Risk 3. Manager until agreement reached or no more progress possible, involve a team of SMEs as necessary. 4. NG9-1-1 Entity Security Risk Manager signs EA/RAF. 5. The Security POC / Team documents concurrence position and signs the form 6. NG9-1-1 Entity Risk Acceptance Approver (senior manager) reviews the form, determines/documents strategy and reason, ensures risk mitigation is completed on the form, and accepts full responsibility and accountability by signing the EA/RAF. 7. The Security Risk Manager shall ensure the completed EA/RAF along with all necessary signatures/approvals, either physical or electronic, are filed with the reviewing Security POC / Team. 8. The Security Risk Manager, Security POC / Team, and Risk Acceptance Approver as well as other involved parties	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 5 - Exception Request / Risk Assessment

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
204	12.3.2	The entity tracks and documents risks in accordance with the chart provided in Appendix A.	R	☐ C ☐ No ☐ N/A	
205	12.4	Risk assessments are reviewed periodically in compliance with the following timeframes: • Critical 0 Months • High 3 Months • Medium 6 Months • Low 12 Months	R	☐ C ☐ No ☐ N/A	
206	12.5	Any change to the circumstances identified in the EA/RAF that affect the associated risk is immediately documented and submitted through the EA/RAF process.	R	☐ C ☐ No ☐ N/A	
207	12.6.1-.3	When conducting risk assessments, vulnerability assessments, and impact assessments they should be conducted using the guidance provided in sections 12.6Risks are identified and assessed IAW Para 12.6.1 through 12.6.3.	BP	☐ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 5 - Exception Request / Risk Assessment

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
208	12.6.8	The EA/RAF should comply with the requirements of Para 12.6.8.	BP	■ C ☐ No ☐ N/A	

Section 5 - Exception Request / Risk Assessment Auditor: Ed Vea Date: 1/15/2019 _____

One Nation 9-1-1 One Number

Section 6 - Hiring Practices

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
209	4.2	Does the organization have a Hiring Practice Policy?	R	■ C ☐ No ☐ N/A	

Section 6 - Hiring Practices Auditor: Ed Vea Date: 1/15/2019 _____

One Nation 9-1-1 One Number

Section 7 - Incident Response

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
210	13 & 4.2	Has a formal, written Incident Response Plan detailing how the organization will respond to a computer security incident been created?	R	■ C ☐ No ☐ N/A	
211	7.2.6	Are software and/or data changes initiated due to outage/recovery process documented and retained until it is determined the production system and data were not corrupted?	R	■ C ☐ No ☐ N/A	
212	7.5.5	Have Business Continuity/Disaster Recovery (BC/DR) procedures been developed and tested?	R	■ C ☐ No ☐ N/A	
213	7.5.5	Do the plans allow for the 'Worst Case' event (i.e. Incident Recovery outside 50 miles from normal location)?	R	■ C ☐ No ☐ N/A	
214	7.5.5	Are BC/DR drills conducted at least annually?	R	■ C ☐ No ☐ N/A	

Section 7 - Incident Response Auditor: Ed Vea _____ Date: 1/15/2019

One Nation 9-1-1 One Number

Section 8 - Information Classification and Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
215	5	Does the organization have an Information Classification and Protection Policy that encompasses both administrative and production systems?	BP	☐ C ☐ No ☐ N/A	
216	5.10.1	Does the organization have disposal procedures for hard copy or printed sensitive data?	BP	☐ C ☐ No ☐ N/A	
217	5.10.2	Does the organization have sanitation procedures for media/devices containing sensitive data?	BP	☐ C ☐ No ☐ N/A	
218	5.2.1	Have Data **Owner** responsibilities been defined?	BP	☐ C ☐ No ☐ N/A	
219	5.2.2	Have Data **Custodian** responsibilities been defined?	BP	☐ C ☐ No ☐ N/A	
220	5.2.3	Are Data Classifications defined and used?	BP	☐ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 8 - Information Classification and Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
221	5.4.6	Is sensitive data received from a third party treated as if it were internal sensitive data?	BP	■ C ☐ No ☐ N/A	
222	5.5	When receiving information where the classification of information is unknown, does the organization treat it as Sensitive (Internal Use Only) until the proper classification is determined or it is determined to be Public Information by the originator or other applicable laws and regulations?	BP	■ C ☐ No ☐ N/A	
223	5.6	Does the organization protect classified information from unauthorized access?	BP	■ C ☐ No ☐ N/A	
224	5.7	Does the organization encrypt stored or transmitted classified information using AES Encryption Algorithm?	BP	■ C ☐ No ☐ N/A	
225	5.7	Does the organization have a policy for removing Mobile Computing Devices with classified data from the NG9-1-1 Entity?	BP	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 8 - Information Classification and Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
226	5.8	Does the entity utilize recorded/certified delivery for transporting sensitive data or media/devices containing sensitive data?	BP	■ C ☐ No ☐ N/A	

Section 8 - Information Classification and Protection Auditor: Ed Vea Date: 1/15/2019 _____

One Nation 9-1-1 One Number

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
227	4.2	Does the organization have a Physical Security Policy?	R	■ C ☐ No ☐ N/A	
228	6.5	Does the Public Safety entity require annual Security Awareness Training?	R	■ C ☐ No ☐ N/A	
229	6.5	Have all Public Safety employees completed the annual Security Awareness Training?	R	■ C ☐ No ☐ N/A	
230	6.6	Does the entity have procedures for reporting any suspicious or unusual activity which may indicate an attempt to breach the Public Safety networks and systems?	R	■ C ☐ No ☐ N/A	
231	8	Is the entity is physically secured and protected from theft, misappropriation, misuse, and unauthorized access, and damage?	R	■ C ☐ No ☐ N/A	
232	8.1	Doors with security mechanisms shall not be propped open.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
233	8.1	Employees, suppliers, contractors and agents authorized to enter a controlled physical access area shall not allow unidentified, unauthorized or unknown persons to follow them through a controlled access area entrance.	R	■ C ☐ No ☐ N/A	
234	8.1	Each person entering a controlled access facility shall follow the physical access control procedures in place for that facility.	R	■ C ☐ No ☐ N/A	
235	8.1	Personnel shall be vigilant while inside the building and challenge and/or report unidentified persons including persons not displaying identification badges who have gained access.	R	■ C ☐ No ☐ N/A	
236	8.1	When automated access control and logging devices are installed, personnel shall use them to record their entry and exit.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
237	8.2.1	Personnel authorized with reoccurring unescorted access do not loan or share physical access devices or codes with another person?	R	■ C ☐ No ☐ N/A	
238	8.2.1.1	Non-employees granted reoccurring access are sponsored by NG9-1-1 management personnel?	R	■ C ☐ No ☐ N/A	
239	8.2.1.1	Does the facility's Physical Security Policy comply with all federal, state, and local laws?	R	■ C ☐ No ☐ N/A	
240	8.2.1.2	Identification badges containing a picture of the holder shall be issued to all residents of buildings containing information resources.	R	■ C ☐ No ☐ N/A	
241	8.2.1.2	Are ID Badges with picture issued to all residents of buildings containing information resources	R	■ C ☐ No ☐ N/A	
242	8.2.1.2	If the facility is guarded, identification badge is displayed to the guard on entry?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
243	8.2.1.2	Are persons on NG9-1-1 Entity premises required to present identification badges for examination and/or validation upon request?	R	■ C ☐ No ☐ N/A	
244	8.2.1.2	Building residents and non-residents with reoccurring access who do not have a valid identification badge in their possession are signed in and vouched for by an authorized building resident who possesses and displays a valid picture identification badge?	R	■ C ☐ No ☐ N/A	
245	8.2.1.2	Are temporary identification badge issued to all persons who do not have a permanent identification badge when entering the facility?	R	■ C ☐ No ☐ N/A	
246	8.2.1.2	Are persons who do not have a permanent identification badge escorted while in the facility?	R	■ C ☐ No ☐ N/A	
247	8.4.1	All portable computing devices in work areas are kept physically secure?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
248	8.4.1	When equipped with locks, portable computing devices are kept locked to prevent theft.	R	■ C ☐ No ☐ N/A	
249	8.4.1	Keys are stored in a secure location	R	■ C ☐ No ☐ N/A	
250	8.4.1	Docking station style portable devices are stored in a secure location when not in use.	R	■ C ☐ No ☐ N/A	
251	8.4.1	Docking station style portable devices are not left unattended outside normal working hours even when in the docking station	R	■ C ☐ No ☐ N/A	
252	8.4.1	Other portable devices are stored in a locked cabinet, drawer, or office (not just the building) when not in use	R	■ C ☐ No ☐ N/A	
253	8.4.1	Extra security precautions are implemented in and around the receiving, staging, assembly, and storage areas used for large deployments of portable computing devices	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
254	8.4.2	Vigilance is maintained in airport luggage inspection and transfer areas, hotel check in and checkout areas and other public areas	R	■ C ☐ No ☐ N/A	
255	8.4.2	Devices are not left unattended in conference rooms, etc.	R	■ C ☐ No ☐ N/A	
256	8.4.2	Devices are not exposed to extreme heat or cold.	R	■ C ☐ No ☐ N/A	
257	8.5	Information resources are protected by a UPS system and/or a 'mirrored site' second location not subject to the same power outage.	R	■ C ☐ No ☐ N/A	
258	8.5	All buildings and critical support facilities have protective physical measures in place.	R	■ C ☐ No ☐ N/A	
259	8.6.1	Server Rooms, Data Centers, Wire Closets, and any other critical locations have limited and controlled access 24/7/365.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
260	8.6.1	Raised floors or suspended ceilings do not allow physical access to limited access areas.	R	■ C ☐ No ☐ N/A	
261	8.6.2.1	The facility has a fire protection/detection system which meets code and is maintained and inspected at regular intervals.	R	■ C ☐ No ☐ N/A	
262	8.6.2.2	If sprinkler systems are provided, fire retardant polyethylene sheeting is readily available to protect media and equipment.	R	■ C ☐ No ☐ N/A	
263	8.6.2.4	Cooling equipment is installed and in good working order.	R	■ C ☐ No ☐ N/A	
264	8.6.2.5	HVAC systems are used to maintain environmental conditions meeting manufacturer's requirements and are supported by backup power systems dedicated.	R	■ C ☐ No ☐ N/A	
265	8.7.1	Network equipment and access to cabling and physical wiring infrastructure are secured with appropriate physical access controls.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
266	8.7.2	Active network jacks and connections are located only in physically secured locations (i.e., entity owned or leased space, in locked cabinets, or protected by locked physical barriers).	R	■ C ☐ No ☐ N/A	
267	8.7.3	Unused network connections are disabled or removed in a timely manner.	R	■ C ☐ No ☐ N/A	
268	8.7.4	Network Media are selected and located so as to minimize the possibility of wiretapping, eavesdropping, or tampering.	R	■ C ☐ No ☐ N/A	

Section 9 - Physical Security Auditor: Ed Vea Date: 1/15/2019 _____

One Nation 9-1-1 One Number

Section 10 - Compliance Audits & Reviews

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
269	11	Internal audits are, at minimum, conducted annually.	R	■ C ☐ No ☐ N/A	
270	11	Findings from such assessments are subject to corrective actions and are applied to the satisfaction of the auditing entity.	R	■ C ☐ No ☐ N/A	
271	11	External security audits are conducted at a minimum, once every 3 years	R	■ C ☐ No ☐ N/A	
272	11	Security audits utilize various methods to assess the security of networks and processes, applications, services, and platforms Suggested methods include automated tools, checklists, documentation review, penetration testing, and interviews	R	■ C ☐ No ☐ N/A	

Section 10 - Compliance Audits & Reviews Auditor: Ed Vea Date: 1/15/2019 _____

One Nation 9-1-1 One Number

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
273	7.2.8.1	Before deployment of new forms of communication, a risk assessment should be conducted in accordance with: • The impact of resource availability • The business justification or importance of the service or data to use a specific communication method. The utility of the service compared to the security risk • The false positive rate (e.g. the possibility this new form of communication can generate false alarms while there are no security vulnerabilities) • The false negative rate (e.g. the potential of unknown new vulnerability is introduced by this new technology while the vulnerabilities are undetected) • The legal status (e.g. liability, contract language, recording as evidence, authority to access information, and privacy limitations) • The volume (normal, bandwidth, latency, diversity/redundancy induced denial of service etc.)	BP	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
274	4.2	Does the organization have a Remote Access Policy?	R	■ C ☐ No ☐ N/A	
275	9	No remote access is permitted to any NG9-1-1 Entity unless addressed by contract, employee policy, or similar legal instrument which contains adequate security language as determined by a security professional?	R	■ C ☐ No ☐ N/A	
276	9.1	Networks are segmented by business and technical functions to allow appropriate levels of protection be created while not placing unneeded restrictions on lesser risk areas	R	■ C ☐ No ☐ N/A	
277	9.1	All boundaries and points of ingress and egress are clearly defined for each network?	R	■ C ☐ No ☐ N/A	
278	9.1.1	Firewalls have been established at all boundary points to control traffic in and out? .	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
279	9.1.1	Firewalls use "fail all" as default?	R	■ C ☐ No ☐ N/A	
280	9.1.1	Application Layer Firewalls are in use (recommended)	BP	■ C ☐ No ☐ N/A	
281	9.1.10	Firewall logs are retained in accordance with applicable information retention requirements?	R	■ C ☐ No ☐ N/A	
282	9.1.10	Logs are replicated off of the firewall?	BP	■ C ☐ No ☐ N/A	
283	9.1.11	Identification, authentication, and access rights to log data are controlled to preserve the chain of custody for evidentiary purposes?	R	■ C ☐ No ☐ N/A	
284	9.1.2	Access through firewalls is governed by an established policy defining clear guidelines for what is or will be allowed?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
285	9.1.3	At a minimum, restriction of source and destination IP addresses are specific to individual addresses?	R	■ C ☐ No ☐ N/A	
286	9.1.3	The security risks for every host or platform within the network range or subnet are evaluated?	R	■ C ☐ No ☐ N/A	
287	9.1.4	The Firewall Administrator has minimized the number of ports exposed or permitted though the firewall? Clarifying note: the firewall administrator should be employing the least-access necessary privilege to ensure that only the necessary ports required for operation are permitted through the firewall.	R	■ C ☐ No ☐ N/A	
288	9.1.5	All Firewall Administrators are highly qualified and experienced and have an in depth knowledge and/or experience in firewall support and management, various operating systems including application and operating system protocols (ports and sockets), networking, routing, LAN/WAN technologies and	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
		associated security implications? (Auditor Guidance: Qualifications considered are, industry and or vendor certifications with various firewall products)			
289	9.1.6	Is the use of ports used by the operating system or infrastructure functions and features across network boundaries strictly controlled at the firewall?	R	■ C ☐ No ☐ N/A	
290	9.1.7	Firewall rules are reviewed at least once per year to verify continued need?	R	■ C ☐ No ☐ N/A	
291	9.1.8	Firewalls are accessed at least annually to address vulnerabilities identified since the last inspection?	R	■ C ☐ No ☐ N/A	
292	9.1.9	All firewalls must log traffic with at minimum, source and destination addresses and ports are captured along with relevant time stamps and actions by the firewall.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
293	9.2	No remote access is allowed to any NG9-1-1 Entity unless addresses by contract, employee policy, or similar legal instrument which contains adequate security language as determined by a security professional	R	■ C ☐ No ☐ N/A	
294	9.2.1	Client based VPNs and/or consolidated modem pools are operated by NG9-1-1 Entity security personnel or personnel contracted for the purpose.	R	■ C ☐ No ☐ N/A	
295	9.2.1	Strict control is maintained for the VPN and/or consolidated modem infrastructures as they enable access to the NG9-1-1 Entity from public networks such as the Internet or public switched telephone network	R	■ C ☐ No ☐ N/A	
296	9.2.1	All client based VPNs utilize industry standard technologies.	R	■ C ☐ No ☐ N/A	
297	9.2.1	All client based VPNs and/or consolidated modem pools access utilize strong authentication which includes single use passwords.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
298	9.2.1	All client based VPNs and/or consolidated modem pools access are controlled by a Firewall.	R	■ C ☐ No ☐ N/A	
299	9.2.1	All client based VPNs and/or consolidated modem pools access are logged.	R	■ C ☐ No ☐ N/A	
300	9.2.2	If directly attached modems are used, have they been approved using the exception methodology in Section 12?	R	■ C ☐ No ☐ N/A	
301	9.2.2	Directly attached modems utilize industry standard third party authentication schema.	R	■ C ☐ No ☐ N/A	
302	9.2.2	Use of only 'secured modems' is permitted. Uncontrolled use of modems can result in serious vulnerabilities and shall use risk mitigation measures	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
303	9.2.2	When such modems are utilized through approved exception, they meet all criteria established for client based VPN or consolidated modem pools. Including firewall access controls and single use passwords.	R	■ C ☐ No ☐ N/A	
304	9.2.2	An accurate inventory of directly attached modems is maintained.	R	■ C ☐ No ☐ N/A	
305	9.2.2	Other modem technologies which shall be considered include "dial/dial back", only when primary access means is down or attached only to devices which have strong authentication mechanisms.	R	■ C ☐ No ☐ N/A	
306	9.2.2	The use of modems which are directly attached to servers, routers, switches, or other such equipment is strongly discouraged and should be prohibited by default	BP	■ C ☐ No ☐ N/A	
307	9.3.1	When using private facility networks such as T1, DS-2, etc., whenever possible the network technologies should be always considered in lieu of communications over public transport	BP	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
308	9.3.1	Organizations should evaluate the importance of the data traversing the network and determine if encryption is appropriate to meet the necessary privacy levels (note: Use of these network technologies does not necessarily preclude the need for end to end encryption)	BP	■ C ☐ No ☐ N/A	
309	9.3.2	Communications over the Internet must be encrypted using IPSEC or SSL.	R	■ C ☐ No ☐ N/A	
310	9.3.2	If using endpoint authentication it has been implemented using either certificates or similar credentials.	R	■ C ☐ No ☐ N/A	
311	9.3.2	When using Internet protocols, industry standard protocols are to be used with minimum key length of 128 bit.	R	■ C ☐ No ☐ N/A	
312	9.3.3	When external connections are clearly identified as un-trusted, a firewall must be utilized to control communication between the external endpoint or network and the NG9-1-1 environment.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
313	9.3.4	When applications require access from external, public transport (i.e. Internet) they have been placed on a DMZ or employ network based encryption and authentication.	R	■ C ☐ No ☐ N/A	
314	9.4	When using Intrusion Detection / Prevention technologies they shall be positioned on internal networks at strategic locations. Note: use of IPS/IDS is not mandatory.	R	■ C ☐ No ☐ N/A	
315	9.4	When using Intrusion Detection / Prevention technologies, their signatures must be routinely updated with processes that include well defined schedules for signature updates and emergency update protocols for high risk and zero day events.	R	■ C ☐ No ☐ N/A	
316	9.5	When used, technologies such as VLAN, VRF, or VPN are classified as required in section 9.3 and once classified they are treated as separate networks.	R	■ C ☐ No ☐ N/A	
317	9.5	All support equipment for virtual or logical networks shall have a management tunnel for support and monitoring.	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
318	9.5	All support equipment for virtual or logical networks limits user group access to the particular virtual facilities when possible.	R	■ C ☐ No ☐ N/A	
319	9.5	Commands (like Telnet), which allow direct access between virtual facilities, are disabled or is only allowed under the highest administrative privilege supported by the device.	R	■ C ☐ No ☐ N/A	
320	9.5	Layer 3 interactions between networks of differing security classifications are only done using a firewall or similar device.	R	■ C ☐ No ☐ N/A	
321	9.5	User access to devices supporting multiple virtual networks should utilize an industry standard authentication and access control protocol such as TACACS or RADIUS.	BP	■ C ☐ No ☐ N/A	

Section 11 - Network / Firewall / Remote Access Auditor: Ed Vea Date: 1/15/2019 _____

One Nation 9-1-1 One Number

Section 12 - Security Enhancement Technical Upgrade

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
322	4.2	Does the organization have a Security Enhancement/Technology Upgrade Policy?	R	■ C ☐ No ☐ N/A	
323	6.7	Do the design, development, administration, and use of any computer resource, network, system, or application always enable compliance with security policies and requirements to its intended use?	R	■ C ☐ No ☐ N/A	
324	6.7	Is incorporating security into new products, services, systems, and networks before they are deployed a priority?	R	■ C ☐ No ☐ N/A	
325	6.7	Is a security assessment of controls and procedures conducted and documented before deployment to certify compliance with security policy and is this document retained as evidence for any future audit?	R	■ C ☐ No ☐ N/A	
326	7.2.8	Is a full business and security assessment conducted for any new form of communications prior to it being connected to the NG 9-1-1 environment?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 12 - Security Enhancement Technical Upgrade

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
327	7.2.8.2	Are communication partners and the full scope of products subjected to full risk assessment?	BP	☐ C ☐ No ☐ N/A	
328	7.2.8.3.1	Are Client Software Add-ons ("plug ins") assessed for security risks?	R	☐ C ☐ No ☐ N/A	
329	7.2.8.3.1	Is client software configured to disallow auto installation of software add-on or plug-ins?	R	☐ C ☐ No ☐ N/A	
330	7.2.8.3.1	Are new add-ons or plug-ins tested prior to installation?	R	☐ C ☐ No ☐ N/A	
331	7.2.8.5	If the NG 9-1-1 Entity uses a VoIP system it does not connect to another VoIP System without securing the connection?	R	☐ C ☐ No ☐ N/A	
332	9.6.1	Network **redundancy** is considered and implemented where possible for On-Site / Local High Availability environments.	R	☐ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 12 - Security Enhancement Technical Upgrade

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
333	9.6.2	Network **diversity** is considered and implemented where possible when implementing NG9-1-1 networks.	R	■ C ☐ No ☐ N/A	
334	9.6.2	Traffic failover between different cities and firewall sites can result in dropping sessions at the time of failure. When employing applications in a network diversity-type model, applications shall be designed to recover such events and users advised to proper "restart" procedures in case such a failover event happens	R	■ C ☐ No ☐ N/A	

Section 12 - Security Enhancement Technical Upgrade

Auditor: Ed Vea Date: 1/15/2019 _____

One Nation 9-1-1 One Number

Section 13 - Technical Solutions Standards

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
335	10	Formalized pre and post security reviews are conducted when changes to architecture, design, or engineering of NG9-1-1 networks.	R	■ C ☐ No ☐ N/A	
336	10	Security reviews are conducted by the NG91-1 security representative and any 3rd party vendors.	R	■ C ☐ No ☐ N/A	
337	10	When changes to architecture, design, or engineering of NG9-1-1 network are made, a formal change control process is followed and appropriate documentation is produced and retained.	R	■ C ☐ No ☐ N/A	
338	10	When architecture, design, or engineering are major, a team of Subject Matter Experts is assembled to review and approve the change.	R	■ C ☐ No ☐ N/A	
339	4.2	Does the organization have a Technology Selection Policy?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 13 - Technical Solutions Standards

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
340	7.4.2	Is time synchronization in accordance with the NENA 04-002 NG9-1-1 Entity Master Clock standard?	R	☐ C ☐ No ☐ N/A	
341	7.4.4	Do formal documented procedures exist for any changes to computer systems and operating systems software?	R	☐ C ☐ No ☐ N/A	
342	7.4.4	Are the procedures identified in the preceding finding followed?	R	☐ C ☐ No ☐ N/A	
343	7.4.4	Is the appropriate level of authorization required and obtained prior to change?	R	☐ C ☐ No ☐ N/A	
344	7.4.4	Does the System Administrator control software changes that affect the operation of an application, operating system, or utilities?	R	☐ C ☐ No ☐ N/A	
345	7.4.4	Does the System Administrator control updates and upgrades that could affect user response, machine performance or operations, security, or system availability?	R	☐ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 13 - Technical Solutions Standards

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
346	7.4.4	Has a detailed audit trail of all modifications to network hardware and software been created, retained, and reviewed at least annually?	R	■ C ☐ No ☐ N/A	
347	7.4.4	Are records of all system/application changes kept at least one year or the last major upgrade whichever is longer?	R	■ C ☐ No ☐ N/A	
348	7.4.4	Do System Controls identify accountability for all program changes to a specific programmer and approving manager?	R	■ C ☐ No ☐ N/A	
349	7.4.4	Excepting reporting procedures are built into the system software to detect computer program, communications and operations failures. .	R	■ C ☐ No ☐ N/A	
350	7.4.4	Are error checking and validation controls are present in software?	R	■ C ☐ No ☐ N/A	
351	7.4.4	Current complete backups are ALWAYS present prior upgrades to provide recovery capability in the event of system problems due to the changes?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 13 - Technical Solutions Standards

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
352	7.4.4	If System Administration or Maintenance is outsourced all records kept by such agencies are available to the NG 9-1-1 Entity?	R	■ C ☐ No ☐ N/A	
353	7.4.5	Have procedures been instituted to verify and document that the business hardware and software are currently supported by the manufacturer or supplier that advisories are issued and fixes are made available for any newly discovered security vulnerability?	R	■ C ☐ No ☐ N/A	
354	7.4.5	Are Temporary Fixes applied when Permanent Fixes are not yet available and are Permanent Fixes applied promptly when they become available?	R	■ C ☐ No ☐ N/A	
355	7.4.5	A process is in place which ensures all applicable Permanent fixes are installed and Temporary Fixes cannot become disabled until Permanent Fixes have been installed?	R	■ C ☐ No ☐ N/A	
356	7.4.5	Are all Permanent or Temporary fixes tested prior to using them in a production environment?	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 13 - Technical Solutions Standards

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
357	7.4.6	Servers, workstations, desktops, or laptops shall be hardened utilizing recognized 'Best Practices for Operating System Hardening' like the National Institute For Standards and Technology (NIST) Guidelines or ISO 2700*x* standards?	R	■ C ☐ No ☐ N/A	
358	7.4.6	All unused services are disabled and end users do not have local administrator rights?	R	☐ C ☐ No ■ N/A	No unused services.
359	7.5.2	Has the entity identified all 'single point of failure' items for their system and have the alternate strategies been planned and documented?	R	☐ C ☐ No ■ N/A	No single point of failure items.
360	7.5.2	Is a plan in place to distribute the 'downtime window' if possible?	R	■ C ☐ No ☐ N/A	
361	7.5.2	Is equipment managed and monitored so if one element is down the entity and management are notified?	R	■ C ☐ No ☐ N/A	
362	7.5.3	Is 'geographic redundancy' available. If so, are procedures in place for activation, use, and testing of the alternate site. Are the results of testing documented	R	■ C ☐ No ☐ N/A	

One Nation 9-1-1 One Number

Section 13 - Technical Solutions Standards

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
363	7.5.3	Are the results of testing of failover procedures documented?	R	■ C ☐ No ☐ N/A	

Section 13 - Technical Solutions Standards Auditor: Ed Vea Date: 1/15/2019 _____

One Nation 9-1-1 One Number

Section 14 - Wireless Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
364	4.2	Does the organization have a Wireless Policy? (Auditor Guidance: if no wireless technologies are in place, then this finding, and all subsequent findings is not applicable All requirements of this document also apply to communications in the 4.9G Hz band)	R	☒ C ☐ No N/A	
365	6.4.6.1	Default router management passwords have been changed and is treated as an Administrator level password for syntax, history, and periodically changed?	R	☒ C ☐ No N/A	
366	6.4.6.1	Router management over wireless link is disabled Router management uses an encrypted protocol?	R	☒ C ☐ No N/A	
367	6.4.6.1	The SSID has been changed from the Default value to an identifier not easily associated with the NG 9-1-1 or easily guessed	R	☒ C ☐ No N/A	

One Nation 9-1-1 One Number

Section 14 - Wireless Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
368	6.4.6.1	SSID broadcast is disabled?	R	[X] C ☐ No N/A	
369	6.4.6.1	Wireless encryption is enabled WPA or greater is used? (Auditor Guidance: WEP is not allowed)	R	[X] C ☐ No N/A	
370	6.4.6.1	The TKIP passphrase is non-trivial and meets the requirements of this document?	R	[X] C ☐ No N/A	
371	6.4.6.1	The rekey maximum is no greater than 3600 seconds?	R	[x] C ☐ No N/A	
372	6.4.6.1	The WIFI LAN is dedicated to the NG 0-1-1 entity and not shared with any other entity?	R	[X] C ☐ No N/A	

One Nation 9-1-1 One Number

Section 14 - Wireless Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
373	6.4.6.1	Media Access Control (MAC) address filters are enabled and MAC Filter List is reviewed at least monthly and immediately after a machine is retired from the network?	R	[X] C ☐ No N/A	
374	6.4.6.1	Ad hoc modes are disabled?	R	[X] C ☐ No N/A	
375	6.4.6.1	Users should be authenticated to the wireless LAN using a two factor mechanism or emerging authentication standards like 802.1x?	BP	[X] C ☐ No N/A	
376	6.4.6.1	The WIFI LAN should be separated from other networks by a firewall which limits access to and from the wireless network on an exception only basis.	BP	[X] C ☐ No N/A	
377	6.4.6.1	Use of Intrusion Detection Systems (IDS) is encouraged on WIFI LANs	BP	[X] C ☐ No N/A	
378	6.4.6.1	Maximum encryption key lengths supported by the device should be utilized	BP	[X] C ☐ No N/A	

One Nation 9-1-1 One Number

Section 14 - Wireless Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
379	6.4.6.1	The WIFI LAN hardware should utilize a third party authentication service for management(such as TACAS, Radius) when supported	BP	[X] C ☐ No N/A	
380	6.4.6.1	The default SSID channel should be changed from its default value	BP	[X] C ☐ No N/A	
381	6.4.6.1	If DHCP is used, automatic assignment of other services(e.g. DNS servers, WINS servers) is allowed and should be reviewed in concert with the overall security plan	BP	[X] C ☐ No N/A	
382	6.4.6.1	DHCP should be disabled and require static IP Addresses for connected devices. If DHCP must be used the DHCP scope(range of addresses) should be kept to a minimum	BP	[X] C ☐ No N/A	
383	6.4.6.1	The WIFI LAN should utilize a Network Access Control technology to ensure proper patching and malicious software screening is performed on all LAN assets. At minimum, use of a rogue machine device detection capability is strongly recommended.	BP	[x] C ☐ No N/A	

One Nation 9-1-1 One Number

Section 14 - Wireless Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
384	6.4.6.2	Bluetooth shall not be used for backup of any medium or device which contains sensitive (internal data only) or greater data.	R	[X] C ☐ No N/A	
385	6.4.6.2	If Bluetooth is used is shall be configured to require device identifiers.	R	[x] C ☐ No N/A	
386	6.4.6.2	Presence of frequency hopping, phase shifting, device serialization, or other technologies alone shall not satisfy encryption or identification requirements	R	[X] C ☐ No N/A	
387	6.4.6.2	Bluetooth wireless networks should be avoided, where possible, including wireless headsets and other human interface devices such as mice and keyboards	BP	[x] C ☐ No N/A	
388	6.4.6.3	Does the entity use the 4.9 MHz band spectrum licensed by the FCC?	R	[X] C ☐ No N/A	
389	6.4.6.3	If the 4.9 MHz band is used are all communications encrypted and all authentication, authorization, and accountability policies complied with?	R	[X] C ☐ No N/A	

One Nation 9-1-1 One Number

Section 14 - Wireless Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
390	6.4.6.3	If the 4.9 MHz band is used a Firewall is deployed at the network boundary	R	[X] C ☐ No N/A	
391	6.4.6.3	All communications on the 4.9G Hz band should be encrypted?	BP	[X] C ☐ No N/A	
392	6.4.6.3	Authentication, authorization, and accountability should be maintained.	BP	[X] C ☐ No N/A	
393	6.4.6.4	Each of these technologies(i.e. 3G, EDGE, etc.) should be regarded as a "remote access" capability and all security standards relevant to remote access found in this document are applicable	R	[X] C ☐ No N/A	
394	6.5	Does the NG 9-1-1 entity require contracting agencies to hold specific or certain certifications to prove compliance with this requirement?	R	[X] C ☐ No N/A	

One Nation 9-1-1 One Number

Section 14 - Wireless Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
395	6.5	Entities responsible for system and security administration (including those contracted to do such tasks) employ individuals who have received current security training on their assigned systems.	R	[X] C ☐ No N/A	
396	6.5	All Public Safety employees receive complete security awareness training as established by each Public Safety Organization on an annual basis?	R	[X] C ☐ No N/A	

Section 14 – Wireless Security Auditor: Ed Vea Date: 1/15/2019 _____

Auditor Comments:

V

Auditor Notes

Auditor Instructions:

One Nation 9-1-1 One Number

4 Appendices

Appendix A: Exception Risk Approval / Mitigation Timeframe Table

Risk Category / Severity	Time to Eliminate Risk	Risk Exists Less Than the Specified Timeframe and Minimum Required Level of Tracking	Risk Exists More Than the Specified Timeframe and Minimum Required Level of Tracking
Critical	Immediate action is required	Escalate until resolved	Escalate until resolved
High	30 days	Security POC / Team and all involved parties shall be kept informed of progress and Risk Acceptance Approver to be made aware by Security POC / Team	Full Documentation and Approval
Medium	60 days	Security POC / Team and all involved parties shall be kept informed of progress	Full Documentation and Approval
Low	90 days	Security POC / Team and all involved parties shall be kept informed of progress	Full Documentation and Approval

5 Recommended Reading and References

It is recommended that the user of this document be very knowledgeable with:

- NENA 75-001 - NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)